CCNA ICND2

Guía Oficial para el examen de Certificación

Segunda edición

Incluye vídeos de aprendizaje

- ✓ Domine los temas del examen **ICND2 640-816** y **CCNA 640-802** con esta guía de estudio oficial.
- ✓ Ponga a prueba su conocimiento con los **cuestionarios que abren los capítulos.**
- ✓ Repase los conceptos clave con los **ejercicios para la preparación del examen.**

ciscopress.com

Wendell Odom, CCIE® No. 1624

CCNA ICND2

Guía Oficial para el examen de Certificación

Segunda edición

CCNA ICND2

Guía Oficial para el examen de Certificación

Segunda edición

Wendell Odom
CCIE® N.º 1624

Wendell ODOM
CCNA ICND2. Guía Oficial para el examen de Certificación. Segunda edición

Todos los derechos reservados.

Queda prohibida, salvo excepción prevista en la ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual *(arts. 270 y sgts.* Código Penal).

De esta edición:
© 2008, PEARSON EDUCACIÓN, S.A.
Ribera del Loira, 28
28006 Madrid (España)

ISBN: 978-84-8322-443-4
Depósito Legal: M-

Authorized translation from the English language edition, entitled *CCNA ICND2. Official Exam Certification Guide. (CCNA Exams 640-816 and 640-802). Second Edition* by Wendell Odom, published by Pearson Education, Inc, publishing as Cisco Press, Copyright © 2008, Cisco Systems, Inc.

All right reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

Spanish language edition published by PEARSON EDUCACIÓN S. A., Copyright © 2008.

Traducido de *CCNA ICND2. Official Exam Certification Guide. (CCNA Exams 640-816 and 640-802). Second Edition*. Wendell Odom. Copyright © 2008, Cisco Systems, Inc. ISBN: 978-1-58720-181-3

Equipo editorial:
Editor: Jesús Domínguez
Técnico editorial: Susana Canedo

Equipo de producción:
Director: José Antonio Clares
Técnico: Diego Marín

Cubierta: Equipo de diseño de Pearson Educación, S.A.
Composición: Ángel Gallardo Serv. Gráf., S.L.
Impreso por:

Nota sobre enlaces a páginas web ajenas: Este libro puede incluir enlaces a sitios web gestionados por terceros y ajenos a PEARSON EDUCACIÓN S. A. que se incluyen sólo con finalidad informativa. PEARSON EDUCACIÓN S. A. no asume ningún tipo de responsabilidad por los daños y perjuicios derivados del uso de los datos personales que pueda hacer un tercero encargado del mantenimiento de las páginas web ajenas a PEARSON EDUCACIÓN S. A y del funcionamiento, accesibilidad o mantenimiento de los sitios web no gestionados por PEARSON EDUCACIÓN S. A. Las referencias se proporcionan en el estado en que se encuentran en el momento de publicación sin garantías, expresas o implícitas, sobre la información que se proporcione en ellas.

IMPRESO EN ESPAÑA - *PRINTED IN SPAIN*

Este libro ha sido impreso con papel y tintas ecológicos

Advertencia y renuncia de responsabilidades

Este libro se ha diseñado para ofrecer información relativa a los exámenes de Cisco ICND1 (640-822), ICND2 (640-816) y CCNA (640-802). Se ha intentado por todos los medios conseguir que este libro sea tan completo y preciso como fuera posible, pero esto no implica ninguna garantía o adecuación.

La información se ofrece "tal y como es". Los autores, Cisco Press y Cisco Systems, Inc. niegan toda responsabilidad frente a toda persona o entidad respecto a posibles pérdidas o daños que surjan de la información contenida en este libro, o del uso de los discos o programas que puedan acompañarlo.

Las opiniones que se expresan en este libro son las del autor, y no coinciden necesariamente con las de Cisco Systems, Inc.

Reconocimiento de marcas registradas

Todos los términos mencionados en este libro de los cuales se sabe que son marcas registradas o comerciales se han escrito en mayúsculas adecuadamente. Cisco Press o Cisco Systems, Inc. no pueden confirmar la exactitud de esta información. El uso de un término en este libro no debe considerarse como algo que afecte a la validez de ninguna marca registrada o comercial.

Acerca del autor

Wendell Odom, CCIE N.º 1624, está en la industria de las redes desde 1981. En la actualidad, imparte cursos de QoS, MPLS y CCNA para Skyline Advanced Technology Services (http://www.skyline-ats.com). Wendell ha trabajado también como ingeniero de redes, asesor, ingeniero de sistemas y como instructor y desarrollador de cursos. Es el autor de todas las ediciones anteriores de *CCNA Exam Certification Guide*, así como de *Cisco QoS Exam Certification Guide*, Segunda Edición, *Computer Networking First-Step*, *CCIE Routing and Switching Official Exam Certification Guide*, Segunda Edición, y de *CCNA Video Mentor*, todos ellos publicados por Cisco Press.

Acerca de los revisores técnicos

Teri Cook (CCSI, CCDP, CCNP, CCDA, CCNA, MCT, y MCSE 2000/2003: Security) tiene más de 10 años de experiencia en la industria de las TI. Ha trabajado con distintos tipos de organizaciones en el sector privado y en Defensa, aportando su gran experiencia técnica en redes y en seguridad para el diseño e implementación de entornos complejos de computación. Desde que obtuvo sus certificaciones, Teri ha estado comprometida con el intento de aportar una formación de calidad en TI a profesionales de TI como instructora. Es una instructora excelente, que utiliza sus experiencias del mundo real para presentar complejas tecnologías de redes. Como instructora de TI, Teri lleva impartiendo clases de Cisco desde hace más de cinco años.

Stephen Kalman es un instructor de seguridad de datos y el autor o editor técnico de más de 20 libros, cursos y títulos de CBT. Su último libro es *Web Security Field Guide*, publicado por Cisco Press. Además de estas responsabilidades, dirige una asesoría, Esquire Micro Consultants, que está especializada en estimaciones de seguridad en redes y en investigaciones *post mortem*.

Stephen Kalman posee las certificaciones SSCP, CISSP, ISSMP, CEH, CHFI, CCNA, CCSA (Checkpoint), A+, Network+ y Security+, y es miembro de la New York State Bar.

Dedicatorias

Para mi maravillosa, adorable y generosa esposa. Gracias por todo tu apoyo, ánimo, amor y respeto.

Agradecimientos

El equipo que ha ayudado a producir este libro es sencillamente tremendo. Todos los que han estado en contacto con el libro lo han mejorado, y el equipo ha sido especialmente bueno en lo tocante a ayudarme a detectar los errores que siempre acaban por aparecer en el manuscrito.

Tanto Teri como Steve han realizado muy bien su trabajo de editores técnicos. La capacidad de Teri para ver todas las frases en el contexto de todo un capítulo, o de todo el libro, era insuperable, y servía de ayuda para detectar cosas que de otro modo nadie detectaría. Steve, como de costumbre, lo hizo de maravilla (después de todo ya ha revisado cinco o seis de mis libros) y, como de costumbre también, aprendo mucho sin más que leer las indicaciones de Steve. La profundidad de las revisiones que se han hecho para este libro es mejor que cualquiera de mis otros libros gracias a Teri y Steve; ¡muchas gracias!

Drew Cupp tuvo la "oportunidad" de desarrollar uno de mis libros por primera vez desde hace mucho tiempo. Las indicaciones y modificaciones de Drew hicieron maravillas, y un par de ojos descansados puestos en los materiales tomados de la edición anterior del libro hicieron que esas partes resultaran muy beneficiadas. Y todo esto mientras hacía mil cosas más, en medio de una planificación que parecía un torbellino. Drew, ¡muchas gracias por hacer un trabajo excelente!

Los encargados de la producción, maravillosos y prácticamente invisibles, hicieron también su excelente trabajo habitual. Cuando veía la forma en que habían cambiado la forma de expresar algo y pensaba, "Vaya, ¿por qué no lo habré escrito así?", me daba cuenta del tipo de equipo que tenemos aquí en Cisco Press. El proceso de revisión final de texto, figuras y páginas requirió también una buena cantidad de tiras y aflojas; esto fue especialmente cierto para las iniciativas de calidad adicionales que hemos aplicado. ¡Gracias a todos!

Brett Bartow fue una vez más el editor ejecutivo del libro, como en casi todos los libros que he ayudado a escribir. Brett realizó su excelente y paciente tarea habitual, siendo mi abogado en muchos aspectos. Brett, gracias por hacer tantas cosas en tantos niveles para ayudarnos a alcanzar el éxito como equipo.

Adicionalmente, hay varias personas que no tienen influencia directa en el libro, pero que también han colaborado para que salga adelante. Gracias a Frank Knox por las discusiones relativas a los exámenes, por qué son tan difíciles y la forma de afrontar la resolución de problemas. Gracias a Rus Healy por la ayuda prestada con la red inalámbrica. Gracias a los Mikes de Skyline por hacer que mis horarios funcionasen para conseguir que este libro (y el libro de ICND1) llegaran a buen puerto. Y gracias a los equipos de cursos y de exámenes de Cisco por las excelentes comunicaciones iniciales y por nuestras conversaciones relativas a los cambios habidos en los cursos y en los exámenes.

Y como siempre, gracias especiales a mi Señor y Salvador Jesucristo; gracias por ayudarme a descansar en Él ¡aunque estuviera haciendo las revisiones finales de 1400 páginas de manuscrito en unas pocas semanas!

Contenido a primera vista

Prólogo ..... **XXVII**

Introducción ..... **XXVIII**

PARTE I. CONMUTACIÓN DE LANs 3

Capítulo 1. LANs virtuales 5

Capítulo 2. Protocolo de árbol del extensión 57

Capítulo 3. Resolución de problemas de conmutación LAN 109

PARTE II. ENRUTAMIENTO IP 157

Capítulo 4. Enrutamiento IP: rutas estáticas y conectadas 159

Capítulo 5. VLSM y resumen de rutas 197

Capítulo 6. Listas de control de acceso IP 223

Capítulo 7. Resolución de problemas de enrutamiento IP 265

PARTE III. CONFIGURACIÓN Y RESOLUCIÓN DE PROBLEMAS CON LOS PROTOCOLOS DE ENRUTAMIENTO 301

Capítulo 8. Teoría de los protocolos de enrutamiento 303

Capítulo 9. OSPF 341

Capítulo 10. EIGRP 377

Capítulo 11. Resolución de problemas en los protocolos de enrutamiento 409

PARTE IV. REDES DE ÁREA AMPLIA 435

Capítulo 12. WANs punto a punto 437

Capítulo 13. Conceptos de Frame Relay 461

Capítulo 14. Configuración y resolución de problemas de Frame Relay 489

Capítulo 15. Redes privadas virtuales 529

PARTE V. ESCALADO DEL ESPACIO DE DIRECCIONES IP 547
Capítulo 16. Conversión de direcciones de red 549
Capítulo 17. IP Versión 6 581

PARTE VI. PREPARACIÓN FINAL 625
Capítulo 18. Preparación final 627

PARTE VII. APÉNDICES 635
Apéndice A. Respuestas de los cuestionarios "Ponga a prueba sus conocimientos" .. 637
Apéndice B. Tabla de conversión de binario a decimal 651
Apéndice C. Actualizaciones del examen ICND2: Versión 1.0 655
Glosario 659
Índice alfabético 679

PARTE VIII. DISPONIBLE SÓLO EN DVD
Apéndice D. Prácticas de subredes
Apéndice E. Páginas de referencia de subredes
Apéndice F. Escenarios adicionales
Apéndice G. Referencia del escenario de vídeo
Apéndice H. Capítulo 12 de ICNDI: Direc cionamiento y *subnetting* IP
Apéndice I. Capítulo 17 de ICNDI: Configuración WAN
Apéndice J. Tablas de memoria
Apéndice K. Clave de respuesta para las tablas de memoria
Apéndice L. Preguntas de respuesta abierta ICND2

Índice de contenido

Prólogo ..... **XXVII**

Introducción ..... **XXVIII**

PARTE I. CONMUTACIÓN DE LANs **3**

Capítulo 1. LANs virtuales **5**

Cuestionario "Ponga a prueba sus conocimientos" 5
Temas fundamentales 8
Conceptos de LANs virtuales 9
Trunking con ISL y 802.1Q 10
ISL 12
IEEE 802.1Q 12
Comparación de ISL con 802.1Q 13
Subredes IP y VLANs 14
Protocolo de *Trunking* VLAN (VTP, *VLAN Trunking Protocol*) 15
Operación normal de VTP utilizando los modos servidor y cliente de VTP 16
Tres requisitos para que VTP funcione entre dos switches 18
Cómo evitar VTP empleando el modo transparente de VTP 19
Almacenamiento de la configuración de la VLAN 19
Versiones de VTP 20
Pruning VTP 21
Resumen de las características de VTP 22
Configuración y verificación de la VLAN y del *trunking* VLAN 23
Creación de VLANs y asignación de VLANs de acceso a una interfaz 23
Configuración del *truking* VLAN 28
Control de las VLANs soportadas en un troncal 32
Trunking para los teléfonos IP de Cisco 34
VLANs y troncales seguros 36
Configuración y verificación de VTP 36
Uso de VTP: configuración de servidores y clientes 37
Advertencias al cambiar la configuración predeterminada de VTP 41
Formas de evitar VTP: configuración del modo transparente 42
Resolución de problemas de VTP 42
Forma de averiguar por qué no funciona correctamente VTP 43
Problemas cuando se conectan nuevos switches y surgen troncales 48
Forma de evitar problemas de VTP mediante procedimientos comprobados 50
Ejercicios para la preparación del examen 51
Repaso de los temas clave 51
Complete de memoria las tablas y las listas 52
Definiciones de los términos clave 52
Referencias de comandos 52

Capítulo 2. Protocolo de árbol de extensión **57**

Cuestionario "Ponga a prueba sus conocimientos" 57
Temas fundamentales 60
Protocolo de árbol de extensión (IEEE 802.1d) 60
Necesidad del árbol de extensión 61

Qué hace el árbol de extensión IEEE 802.1d ... 62
Cómo funciona el árbol de extensión ... 64
La ID de puente STP y la BPDU Hello ... 65
Elección del switch raíz ... 66
Elección del puerto raíz de cada switch ... 67
Elección del puerto designado en cada segmento de LAN ... 68
Cómo reaccionar frente a cambios en la red ... 70
Características opcionales de STP ... 73
EtherChannel ... 74
PortFast ... 75
Seguridad en STP ... 75
STP Rápido (IEEE 802.1w) ... 76
Tipos de enlace y contorno RSTP ... 77
Estados de puerto RSTP ... 78
Roles de puerto RSTP ... 79
Convergencia de RSTP ... 80
Comportamiento de tipo contorno y PortFast ... 81
Tipo enlace compartido ... 81
Tipo enlace punto a punto ... 81
Ejemplo de convergencia rápida de RSTP ... 81
Configuración y verificación de STP ... 84
Instancias múltiples de STP ... 84
Opciones de configuración que influyen en la topología del árbol de extensión ... 86
El ID de puente y la extensión del ID de sistema ... 86
Costes de puerto por VLAN ... 87
Resumen de las opciones de configuración de STP ... 88
Verificación del comportamiento predeterminado en STP ... 88
Configuración de costes de puerto de STP y prioridad del switch ... 90
Configuración de PortFast y BPDU Guard ... 93
Configuración de EtherChannel ... 93
Configuración de RSTP ... 95
Resolución de problemas de STP ... 96
Determinación del switch raíz ... 96
Determinación del puerto raíz en los switches que no son raíz ... 98
Determinando el puerto designado en cada segmento de LAN ... 100
Convergencia de STP ... 101
Ejercicios para la preparación del examen ... 103
Repaso de los temas clave ... 103
Complete de memoria las tablas y las listas ... 104
Definiciones de los términos clave ... 104
Referencias de comandos ... 105
Capítulo 3. Resolución de problemas de conmutación LAN ... 109
Cuestionario "Ponga a prueba sus conocimientos" ... 109
Temas fundamentales ... 110
Metodologías generales de resolución de problemas ... 110
Análisis y predicción del funcionamiento normal de la red ... 111
Análisis del plano de datos ... 112
Análisis del plano de control ... 112
Predicción del funcionamiento normal: resumen del proceso ... 114
Aislamiento del problema ... 115
Análisis de la causa raíz ... 116
El mundo real frente a los exámenes ... 117

Resolución de problemas en el plano de datos de conmutación LAN ... 117
Visión general del proceso de envío de conmutación LAN normal ... 117
Paso 1: confirmar los diagramas de red utilizando CDP ... 120
Paso 2: aislar los problemas de interfaz ... 121
Códigos de estado de interfaz y razones de los estados no operativos ... 122
El estado notconnect y las especificaciones de cableado ... 123
Velocidad de la interfaz y problemas con dúplex ... 125
Paso 3: aislar los problemas de filtrado y de seguridad de puerto ... 128
Paso 4: aislar problemas de VLAN y de *trunking* ... 132
Asegurarse de que las interfaces de acceso correctas están en las VLANs correspondientes ... 133
Las VLANs de acceso no se están definiendo o no están activadas ... 134
Identificar los troncales y las VLANs enviadas en esos troncales ... 134
Ejemplo: resolución de problemas del plano de datos ... 136
Paso 1: verificar la exactitud del diagrama utilizando CDP ... 137
Paso 2: buscar problemas de interfaz ... 139
Paso 3: buscar problemas de seguridad de puerto ... 141
Paso 4: buscar problemas de VLAN y de troncales VLAN ... 143
Predicción del funcionamiento normal del plano de datos de conmutación LAN ... 147
PC1 difunde en VLAN 1 ... 147
Ruta de envío: unidifusión de R1 a PC1 ... 150
Ejercicios para la preparación del examen ... 154
Repaso de los temas clave ... 154
Complete de memoria las tablas y las listas ... 155
Temas del examen ICND2 publicados por Cisco que se tratan en esta parte ... 156

PARTE II. ENRUTAMIENTO IP ... 157

Capítulo 4. Enrutamiento IP: rutas estáticas y conectadas ... 159

Cuestionario "Ponga a prueba sus conocimientos" ... 159
Temas fundamentales ... 161
Enrutamiento y direccionamiento IP ... 162
Enrutamiento IP ... 162
Direccionamiento y *subnetting* IP ... 166
Envío IP por la ruta más específica ... 169
DNS, DHCP, ARP e ICMP ... 170
Fragmentación y MTU ... 172
Rutas a subredes conectadas directamente ... 174
Direccionamiento IP secundario ... 174
Soporte de rutas conectadas en la subred cero ... 177
Configuración de ISL y 802.1Q en los routers ... 177
Rutas estáticas ... 180
Configuración de rutas estáticas ... 181
El comando Ping extendido ... 182
Rutas estáticas predeterminadas ... 185
Rutas predeterminadas empleando el comando ip route ... 185
Rutas predeterminadas empleando el comando ip default-network ... 187
Resumen de las rutas predeterminadas ... 188
Enrutamiento con y sin clase ... 189
Resumen del uso de los términos sin clase y con clase ... 189
Comparación del enrutamiento con clase y sin clase ... 190

Ejercicios para la preparación del examen ... 193
Repaso de los temas clave ... 193
Complete de memoria las tablas y las listas ... 194
Definiciones de los términos clave ... 194
Referencias de comandos ... 194
Capítulo 5. VLSM y resumen de rutas ... 197
Cuestionario "Ponga a prueba sus conocimientos" ... 197
Temas fundamentales ... 199
VLSM ... 199
Protocolos de enrutamiento sin clase y con clase ... 201
Subredes VLSM solapadas ... 201
Diseño de un escenario de subredes empleando VLSM ... 203
Adición de una nueva subred a un diseño existente ... 205
Configuración de VLSM ... 207
Resumen manual de ruta ... 208
Conceptos de los resúmenes de ruta ... 208
Estrategias de los resúmenes de rutas ... 212
Ejemplo del "mejor" resumen en Seville ... 213
Ejemplo del "mejor" resumen en Yosemite ... 214
Autoresumen y redes con clase separadas ... 215
Un ejemplo de autoresumen ... 215
Redes con clase separadas ... 216
Soporte del autoresumen y configuración ... 219
Ejercicios para la preparación del examen ... 220
Repaso de los temas clave ... 220
Complete de memoria las tablas y las listas ... 220
Definiciones de los términos clave ... 221
Lectura de los escenarios del Apéndice F ... 221
Referencias de comandos ... 221
Capítulo 6. Listas de control de acceso IP ... 223
Cuestionario "Ponga a prueba sus conocimientos" ... 223
Temas fundamentales ... 226
Listas de control de acceso IP estándar ... 227
Conceptos de las ACLs IP estándares ... 227
Máscaras *wildcard* ... 230
Una alternativa rápida para interpretar máscaras *wildcard* ... 232
Configuración de las listas de acceso IP estándares ... 233
Ejemplo 1 de ACL IP estándar ... 234
Ejemplo 2 de ACL IP estándar ... 236
Listas de control de acceso IP extendidas ... 238
Conceptos de las ACL IP extendidas ... 238
Coincidencias de los números de puerto TCP y UDP ... 240
Configuración de las ACLs IP extendidas ... 243
Ejemplo 1 de listas de acceso IP extendidas ... 244
Ejemplo 2 de listas de acceso IP extendidas ... 246
Avances en la gestión de la configuración de las ACLs ... 247
Listas de acceso IP con nombre ... 247
Edición de ACLs empleando números de secuencia ... 249
Temas varios sobre las ACLs ... 253
Control de acceso por Telnet y SSH empleando ACLs ... 253
Consideraciones de la implementación de una ACL ... 254

Listas de acceso reflexivas ... 255
ACLs dinámicas ... 257
ACLs basadas en tiempos ... 258
Ejercicios para la preparación del examen ... 259
Repaso de los temas clave ... 259
Complete de memoria las tablas y las listas ... 260
Lectura de los escenarios del Apéndice F ... 260
Definiciones de los términos clave ... 260
Referencias de comandos ... 261

Capítulo 7. Resolución de problemas de enrutamiento IP ... 265

Cuestionario "Ponga a prueba sus conocimientos" ... 265
Temas fundamentales ... 265
Los comandos ping y traceroute ... 266
Protocolo de mensajes de control en Internet (ICMP) ... 266
El comando ping, y la petición de eco y la respuesta de eco ICMP ... 267
El mensaje de destino inalcanzable de ICMP ... 267
El mensaje Redirigir de ICMP ... 270
El mensaje de Tiempo excedido de ICMP ... 271
El comando traceroute ... 271
Resolución de problemas en el proceso de envío de paquetes ... 274
Aislamiento de problemas de enrutamiento IP relacionados con los hosts ... 275
Aislamiento de problemas de enrutamiento IP relacionados con los routers ... 277
Escenario de resolución de problemas n.º 1: problemas con la ruta de envío ... 278
Escenario de resolución de problemas n.º 2: problemas con la ruta inversa ... 281
Un proceso de resolución de problemas alternativo para los Pasos 3, 4 y 5 ... 284
Herramientas y pautas para la resolución de problemas ... 284
Perspectivas y herramientas de enrutamiento host ... 285
Pautas para la resolución de problemas en los hosts ... 285
Soporte de IP en switches LAN ... 286
Referencia de show ip route ... 287
Estado de la interfaz ... 288
Problemas de VLSM ... 289
Forma de conocer cuándo se utiliza VLSM ... 289
Configuración de subredes VLSM solapadas ... 289
Síntomas de las subredes solapadas ... 291
Resumen de la resolución de problemas de VLSM ... 293
Redes discontinuas y autoresumen ... 293
Pautas para la resolución de problemas en las listas de acceso ... 294
Ejercicios para la preparación del examen ... 297
Repaso de los temas clave ... 297
Complete de memoria las tablas y las listas ... 298
Definiciones de los términos clave ... 298
Temas de examen ICND2 publicados por Cisco que se tratan en esta parte ... 300

PARTE III. CONFIGURACIÓN Y RESOLUCIÓN DE PROBLEMAS CON LOS PROTOCOLOS DE ENRUTAMIENTO ... 301

Capítulo 8. Teoría de los protocolos de enrutamiento ... 303

Cuestionario "Ponga a prueba sus conocimientos" ... 303
Temas fundamentales ... 306
Descripción del protocolo de enrutamiento dinámico ... 306

Funciones del protocolo de enrutamiento ... 307
Los protocolos de enrutamiento exteriores e interiores ... 309
Comparando IGPs ... 310
Algoritmos de los protocolos de enrutamiento IGP ... 310
Métricas ... 311
Comparaciones de IGP: resumen ... 313
Distancia administrativa ... 313
Características del protocolo de enrutamiento por vector de distancia ... 315
El concepto de una distancia y un vector ... 316
Funcionamiento del vector de distancia en una red estable ... 317
Prevenir bucles del vector de distancia ... 318
Ruta envenenada ... 319
Problema: cuenta hasta infinito en un único enlace ... 320
Horizonte dividido ... 322
Inversa envenenada y actualizaciones activadas ... 324
Problema: cuenta hasta infinito en una red redundante ... 325
El proceso y el temporizador *holddown* ... 328
Resumen del vector de distancia ... 330
Características del protocolo de enrutamiento por estado del enlace ... 330
Construyendo la misma LSDB en todos los routers ... 331
Aplicando la matemática SPF de Dijkstra para encontrar las mejores rutas ... 333
Convergencia con los protocolos por estado del enlace ... 335
Resumen y comparación con los protocolos por vector de distancia ... 335
Ejercicios para la preparación del examen ... 337
Repaso de los temas clave ... 337
Complete de memoria las tablas y las listas ... 338
Definiciones de los términos clave ... 338
Referencias de comandos ... 338
Capítulo 9. OSPF ... 341
Cuestionario "Ponga a prueba sus conocimientos" ... 341
Temas fundamentales ... 344
El protocolo OSPF y su funcionamiento ... 344
Vecinos en OSPF ... 344
Identificación de routers OSPF mediante un ID de router ... 345
Búsqueda de vecinos diciendo Hello ... 345
Problemas potenciales para llegar a hacerse vecinos ... 347
Estados de vecindad ... 348
Intercambio de la base de datos topológica de OSPF ... 349
Visión general del proceso de intercambio de bases de datos de OSPF ... 349
Selección de un router designado ... 350
Intercambio de bases de datos ... 352
Mantenimiento de la LSDB cuando el router es completamente adyacente ... 352
Resumen de los estados de los vecinos ... 353
Construcción de la tabla de enrutamiento IP ... 353
Escalado de OSPF mediante un diseño jerárquico ... 355
Áreas de OSPF ... 356
Ventajas que aportan las áreas en el diseño de OSPF ... 358
Configuración de OSPF ... 359
Configuración de OSPF con una sola área ... 359
Configuración de OSPF con múltiples áreas ... 361
Configuración del ID de router en OSPF ... 364
Temporizadores Hello y muerto de OSPF ... 365

Métrica de OSPF (coste) ... 366
Autenticación en OSPF ... 368
Equilibrado de la carga en OSPF ... 370
Ejercicios para la preparación del examen ... 371
Repaso de los temas clave ... 371
Complete de memoria las tablas y las listas ... 372
Definiciones de los términos clave ... 372
Referencias de comandos ... 372
Capítulo 10. EIGRP ... 377
Cuestionario "Ponga a prueba sus conocimientos" ... 377
Temas fundamentales ... 380
Conceptos y funcionamiento de EIGRP ... 380
Vecinos EIGRP ... 380
Intercambio de información topológica en EIGRP ... 381
Cálculo de las mejores rutas para la tabla de enrutamiento ... 383
Distancia factible y distancia informada ... 385
Precauciones relativas al ancho de banda en enlaces serie ... 385
Convergencia de EIGRP ... 386
Sucesores y sucesores factibles en EIGRP ... 387
El proceso de consulta y respuesta ... 388
Resumen de EIGRP y comparaciones con OSPF ... 389
Configuración y verificación de EIGRP ... 390
Configuración básica de EIGRP ... 390
Métricas, sucesores y sucesores factibles en EIGRP ... 393
Creación y visualización de una ruta sucesora factible ... 395
Convergencia empleando la ruta sucesora factible ... 396
Autenticación en EIGRP ... 397
Rutas máximas y varianza en EIGRP ... 400
Ajuste fino del cálculo de métricas en EIGRP ... 401
Ejercicios para la preparación del examen ... 403
Repaso de los temas clave ... 403
Complete de memoria las tablas y las listas ... 403
Definiciones de los términos clave ... 404
Referencias de comandos ... 404
Capítulo 11. Resolución de problemas en los protocolos de enrutamiento ... 409
Cuestionario "Ponga a prueba sus conocimientos" ... 409
Temas fundamentales ... 410
Perspectivas para la resolución de problemas con los protocolos de enrutamiento ... 410
Interfaces habilitadas para un protocolo de enrutamiento ... 412
Ejemplo de resolución de problemas en una interfaz EIGRP ... 413
Ejemplo de resolución de problemas en una interfaz ... 418
Relaciones de vecindad ... 420
Requisitos de vecindad en EIGRP ... 421
Requisitos de vecindad en OSPF ... 424
Ejemplo 1 de vecindad en OSPF ... 425
Ejemplo 2 de vecindad en OSPF ... 427
El requisito de igualdad de MTU ... 429
Ejercicios para la preparación del examen ... 430
Repaso de los temas clave ... 430
Complete de memoria las tablas y las listas ... 430
Referencias de comandos ... 430
Temas del examen ICND2 publicados por Cisco que se tratan en esta parte ... 434

PARTE IV. REDES DE ÁREA AMPLIA **435**

Capítulo 12. WANs punto a punto **437**

Cuestionario "Ponga a prueba sus conocimientos" 437
Temas fundamentales 440
Conceptos de PPP 440
El campo de protocolo PPP 440
Protocolo para el control del enlace PPP (LCP) 441
Detección de enlaces con bucle 442
Detección de errores mejorada 443
Multienlace PPP 443
Autenticación en PPP 444
Configuración de PPP 446
Configuración básica de PPP 446
Configuración y verificación de CHAP 447
Configuración de PAP 448
Resolución de problemas en enlaces serie 449
Resolución de problemas de capa 1 450
Resolución de problemas de capa 2 451
Fallo de *keepalive* 452
Fallos de autenticación en PAP y CHAP 453
Resolución de problemas de capa 3 455
Ejercicios para la preparación del examen 457
Repaso de los temas clave 457
Complete de memoria las tablas y las listas 457
Definiciones de los términos clave 458
Referencias de comandos 458

Capítulo 13. Conceptos de Frame Relay **461**

Cuestionario "Ponga a prueba sus conocimientos" 461
Temas fundamentales 464
Visión general de Frame Relay 465
Estándares de Frame Relay 467
Circuitos Virtuales 467
LMI y tipos de encapsulación 470
Direccionamiento en Frame Relay 472
Direccionamiento local en Frame Relay 473
Direccionamiento global en Frame Relay 474
Temas de la capa de red relativos a Frame Relay 477
Direccionamiento de capa 3 en Frame Relay: una subred que contiene todos los DTEs de Frame Relay 477
Direccionamiento de capa 3 en Frame Relay: una subred por VC 478
Direccionamiento de capa 3 en Frame Relay: método híbrido 480
Manipulación de la difusión de capa 3 482
Control de la velocidad y de los descartes en la nube Frame Relay 482
FECN y BECN 483
El bit posible para descarte (*Discard Eligibility*, DE) 484
Ejercicios para la preparación del examen 485
Repaso de los temas clave 485
Complete de memoria las tablas y las listas 485
Definiciones de los términos clave 486

Capítulo 14. Configuración y resolución de problemas de Frame Relay **489**
Cuestionario "Ponga a prueba sus conocimientos" 489
Temas fundamentales 492
Configuración y verificación de Frame Relay 492
Planificación de una configuración de Frame Relay 493
Una red de malla completa con una subred IP 494
Configuración de la encapsulación y de LMI 496
Asignación de direcciones en Frame Relay 497
ARP Inverso 500
Mapeo estático en Frame Relay 501
Una red de malla parcial con una subred IP por VC 502
Asignación de un DLCI a una subinterfaz particular 505
Comentarios sobre el direccionamiento global y local 505
Verificación de Frame Relay 506
Una red de malla parcial con partes de malla completa 508
Resolución de problemas en Frame Relay 511
Proceso sugerido para la resolución de problemas de Frame Relay 512
Problemas de capa 1 relativos al enlace de acceso (Paso 1) 513
Problemas de capa 2 relativos al enlace de acceso (Paso 2) 514
Problemas y estado de los PVCs (Paso 3) 516
Búsqueda de la subred conectada y de la interfaz de salida (Pasos 3a y 3b) 517
Búsqueda de los PVCs asignados a esa interfaz (Paso 3c) 518
Determinación del PVC que se usa para llegar a un determinado vecino (Paso 3d) 519
Estado de un PVC 519
Estado de la subinterfaz 521
Problemas de mapeo en Frame Relay (Paso 4) 522
Encapsulación entre extremos (Paso 5) 523
Números de subred desiguales (Paso 6) 524
Ejercicios para la preparación del examen 525
Repaso de los temas clave 525
Complete de memoria las tablas y las listas 525
Lectura de los escenarios del Apéndice F 526
Referencias de comandos 526
Capítulo 15. Redes privadas virtuales **529**
Cuestionario "Ponga a prueba sus conocimientos" 529
Temas fundamentales 531
Fundamentos de VPN 531
VPNs IPsec 534
Encriptación IPsec 535
Intercambio de claves en IPsec 536
Autenticación e integridad de mensajes en IPsec 537
Protocolos de seguridad ESP y AH 539
Consideraciones sobre la implementación de IPsec 540
VPNs SSL 541
Ejercicios para la preparación del examen 544
Repase todos los temas importantes 544
Complete de memoria las tablas y las listas 544
Definiciones de los términos clave 545
Temas del examen ICND2 publicados por Cisco que se tratan en esta parte 546

PARTE V. ESCALADO DEL ESPACIO DE DIRECCIONES IP **547**

Capítulo 16. Conversión de direcciones de red **549**

Cuestionario "Ponga a prueba sus conocimientos" 549
Temas fundamentales 552
Perspectivas sobre la escalabilidad de direcciones en IPv4 552
CIDR 553
Agregación de rutas para lograr tablas de enrutamiento más breves 553
Conservación de direcciones IPv4 555
Direccionamiento privado 555
Conceptos de conversión de direcciones de red 556
NAT estática 557
NAT dinámica 560
Sobrecarga de NAT con la Conversión de direcciones de puerto (*Port Address Translation*, PAT) 561
Conversión de direcciones superpuestas 563
Configuración y resolución de problemas en NAT 565
Configuración de NAT estática 565
Configuración de NAT dinámica 568
Configuración de sobrecarga NAT (PAT) 572
Resolución de problemas de NAT 574
Ejercicios para la preparación del examen 576
Repaso de los temas clave 576
Complete de memoria las tablas y las listas 577
Definiciones de los términos clave 577
Referencias de comandos 577

Capítulo 17. IP Versión 6 ..... **581**

Cuestionario "Ponga a prueba sus conocimientos" 581
Temas fundamentales 583
Direccionamiento de unidifusión global, enrutamiento y subredes 585
Agregación global de rutas para un enrutamiento eficiente 586
Convenciones para la representación de direcciones IPv6 588
Convenciones para escribir prefijos de IPv6 589
Ejemplo de asignación de un prefijo de unidifusión global 592
Creación de subredes con direcciones IPv6 de unidifusión global dentro de una empresa 594
Terminología de prefijos 597
Protocolos y direccionamiento IPv6 597
DHCP para IPv6 598
Asignación de dirección de host IPv6 599
El ID de interfaz IPv6 y el formato EUI-64 599
Configuración estática de direcciones IPv6 601
Autoconfiguración sin estado y publicaciones de los routers 602
Resumen de la configuración de direcciones en IPv6 604
Descubrimiento del router predeterminado mediante NDP 604
Aprendizaje de la dirección o direcciones IP de los servidores DNS 605
Direcciones IPv6 605
Direcciones IPv6 de unidifusión 606
Multidifusión y otras direcciones IPv6 especiales 608
Resumen de los protocolos y el direccionamiento IP 609
Configuración del enrutamiento y de los protocolos de enrutamiento en IPv6 611
Protocolos de enrutamiento IPv6 611

Configuración de IPv6 612
Opciones para la transición a IPv6 615
Pilas duales IPv4/IPv6 616
Túneles 616
Conversión entre IPv4 e IPv6 por medio de NAT-PT 618
Resumen de la transición 618
Ejercicios para la preparación del examen 620
Repaso de los temas clave 620
Complete de memoria las tablas y las listas 621
Definiciones de los términos clave 621
Referencias de comandos 621

PARTE VI. PREPARACIÓN FINAL 625

Capítulo 18. Preparación final 627
Herramientas para la preparación final 627
Cisco CCNA Prep Center 628
Vídeos sobre *subnetting*, páginas de referencia y problemas de práctica 628
Escenarios 629
Plan de estudio 629
Recuerde los hechos 630
Prácticas de *subnetting* 630
Aprenda a resolver problemas empleando escenarios 631
Resumen 632

PARTE VII. APÉNDICES 635

Apéndice A. Respuestas de los cuestionarios "Ponga a prueba sus conocimientos" 637

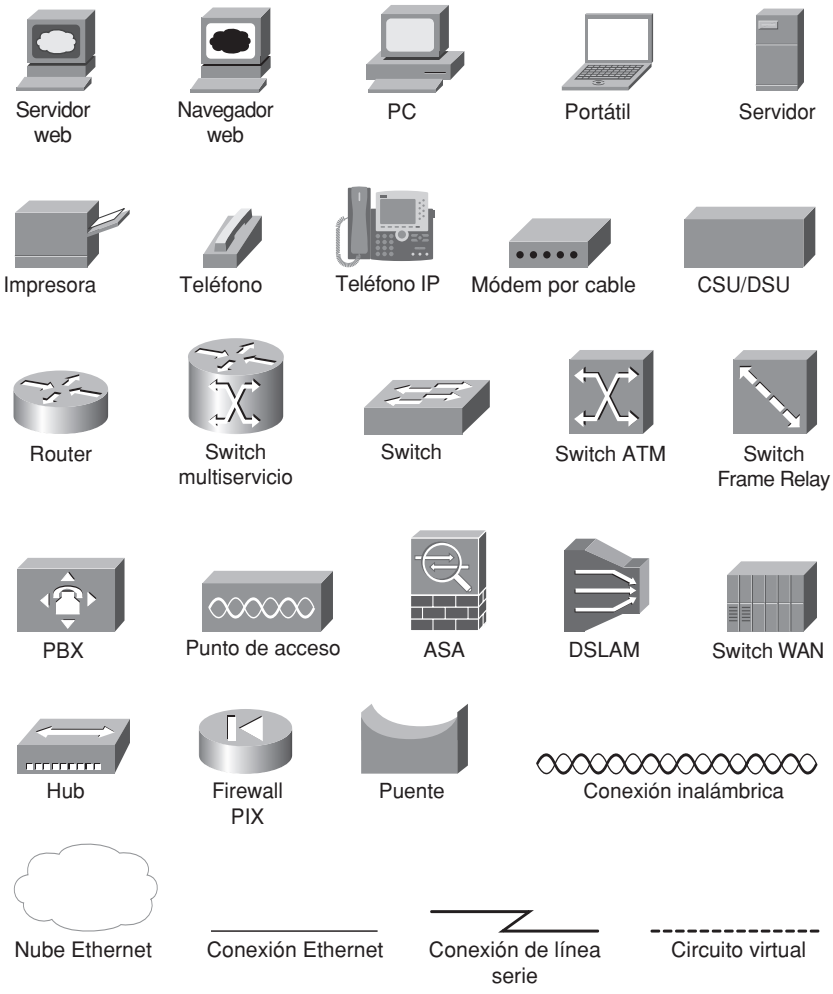
Apéndice B. Tabla de conversión de decimal a binario 651

Apéndice C. Actualizaciones del examen ICND2: Versión 1.0 655

Glosario 659

Índice alfabético 679

Iconos utilizados en este libro



Convenciones sintácticas de los comandos

Las convenciones que se utilizan para presentar la sintaxis de los distintos comandos en este libro son las siguientes:

- `Esta fuente` indica aquellos comandos y palabras reservadas que se escriben literalmente en la forma que se muestra. En los ejemplos reales de configuración, y en sus resultados (no en la sintaxis general de los comandos), `este cambio de fuente` indica aquellos comandos que se introducen manualmente por parte del usuario (como el comando `show`).
- *Cursiva* indica aquellos argumentos para los que el usuario debe proporcionar valores.
- Las barras verticales (|) separan elementos alternativos, mutuamente excluyentes.
- Los corchetes cuadrados [ ] indican elementos opcionales.
- Las llaves { } indican la necesidad de optar por una u otra posibilidad.
- Las llaves entre corchetes cuadrados [{ }] indican la necesidad de optar por una u otra posibilidad dentro de un elemento opcional.

Prólogo

CCNA ICND2 ***Guía Oficial para el examen de Certificación***, Segunda Edición, es un excelente recurso de autoestudio para el examen CCNA ICND2. Al pasar el examen ICND2 se valida el conocimiento y las capacidades necesarios para abordar con éxito la instalación, operación y resolución de problemas de una red de una PYME. Es uno de los dos exámenes que se requieren para la certificación CCNA.

Obtener una certificación en la tecnología de Cisco es clave para el desarrollo educativo continuado de los profesionales de las redes en la actualidad. Mediante sus programas de certificación, Cisco valida las capacidades y experiencia necesarias para administrar de forma efectiva las redes de las empresas modernas.

Las guías de Cisco Press para exámenes de certificación, y los materiales de preparación, ofrecen un acceso excepcional y flexible al conocimiento y a las informaciones necesarias para estar al día en la propia línea de trabajo, o para adquirir nuevas capacidades. Tanto si se utilizan como suplemento para una formación más tradicional como si son la fuente principal de información para el aprendizaje, estos materiales ofrecen a los usuarios la información y la validación de conocimientos necesarios para adquirir una nueva comprensión y más habilidad.

Los libros de Cisco Press, que se desarrollan en conjunción con el equipo de certificación y formación de Cisco, son los únicos libros de autoestudio que cuentan con la autorización de Cisco, y ofrecen a los alumnos una colección de herramientas para practicar con los exámenes, así como materiales que sirven de ayuda para asegurarse de que los principiantes puedan captar totalmente los conceptos e informaciones presentados.

Los *partners* de soluciones de aprendizaje de Cisco ofrecen en todo el mundo, de forma exclusiva, cursos autorizados por Cisco y guiados por un instructor, aprendizaje a distancia, y simulaciones. Para obtener más información, visite http://www.cisco.com/go/training.

Deseamos que encuentre estos materiales una parte útil y enriquecedora de su preparación del examen.

Erik Ullanderson

Manager, Global Certifications

Learning@Cisco

Agosto, 2007

Introducción

¡Enhorabuena! Si ha ido leyendo hasta llegar a la introducción de este libro, es probable que ya haya decidido presentarse a una certificación de Cisco. Si desea tener éxito como técnico en la industria de las redes, necesita conocer a Cisco. Cisco tiene una cuota de mercado espectacular en el mundo de los routers y de los switches, llegando a superar el 80 por cien de cuota de mercado en ciertos entornos. En muchos países y mercados de todo el mundo, al hablar de redes estamos hablando de Cisco. Si desea que le tomen en serio como ingeniero de redes, la certificación de Cisco tiene perfecto sentido.

Desde un punto de vista histórico, la primera certificación de Cisco para el nivel de entrada fue la certificación denominada *Cisco Certified Network Associate* (CCNA), que se ofreció por primera vez en 1998. Las tres primeras versiones de la certificación CCNA (1998, 2000 y 2002) requerían pasar un solo examen para conseguir la certificación. Sin embargo, con el tiempo el examen iba creciendo, tanto en lo tocante a la cantidad de material tratado como en el grado de dificultad de las cuestiones. Como consecuencia, para la cuarta revisión de importancia de los exámenes, anunciada en 2003, Cisco siguió ofreciendo una sola certificación (CCNA), pero proponía dos opciones para los exámenes necesarios para obtenerla: una opción de un solo examen, y otra de dos exámenes. La opción de dos exámenes permitía a los alumnos estudiar aproximadamente la mitad del material, y hacer y aprobar un examen, antes de pasar al siguiente.

Cisco anunció cambios en la certificación CCNA y en los exámenes en junio de 2007. Este anuncio incluye muchos cambios, y especialmente los siguientes:

- En general, los exámenes abarcan un rango de temas más extenso.
- Los exámenes se centran más en comprobar las capacidades del examinado (en lugar de limitarse a comprobar sus conocimientos).
- Cisco ha creado una nueva certificación de nivel de entrada: la certificación *Cisco Certified Entry Network Technician* (CCENT).

Para las certificaciones actuales, que se anunciaron en junio de 2007, Cisco creó los exámenes ICND1 (640-822) e ICND2 (640-816), junto con el examen CCNA (640-802). Para recibir la certificación CCNA, se pueden pasar los exámenes ICND1 e ICND2, o bien se puede pasar solamente el examen CCNA. El examen CCNA se limita a tratar todos los temas de los exámenes ICND1 e ICND2, y ofrece dos opciones para obtener la certificación CCNA. La vía de los dos exámenes ofrece a las personas menos experimentadas la posibilidad de estudiar un temario más reducido, mientras que la opción de un solo examen ofrece una vía de certificación más económica para quienes prefieran preparar todo el temario de una vez.

Aunque la opción de dos exámenes resultará útil para algunos candidatos a la certificación, Cisco ha diseñado el examen ICND1 con un objetivo mucho más importante. La certificación CCNA ha crecido hasta tal punto que comprueba unos conocimientos y capacidades que van más allá de lo que necesitaría un técnico de nivel de entrada. Cisco necesitaba una certificación que reflejase mejor las capacidades necesarias para tareas de redes de nivel de entrada. Por tanto, Cisco diseñó el curso *Interconnecting Cisco Networking*

Devices 1 (ICND1), y el correspondiente examen ICND1 640-822, de tal modo que incluyera el conocimiento y capacidades que son más necesarios para un técnico de nivel de entrada en la red de una pequeña empresa. Y para demostrar que se tienen las capacidades necesarias para esas tareas de nivel de entrada, Cisco ha creado una nueva certificación llamada CCENT, que se obtiene pasando el examen ICND1.

La Figura I.1 muestra la organización básica de las certificaciones y de los exámenes que se emplean para obtener las certificaciones CCENT y CCNA. (Obsérvese que no hay una certificación distinta correspondiente a pasar el examen ICND2.)

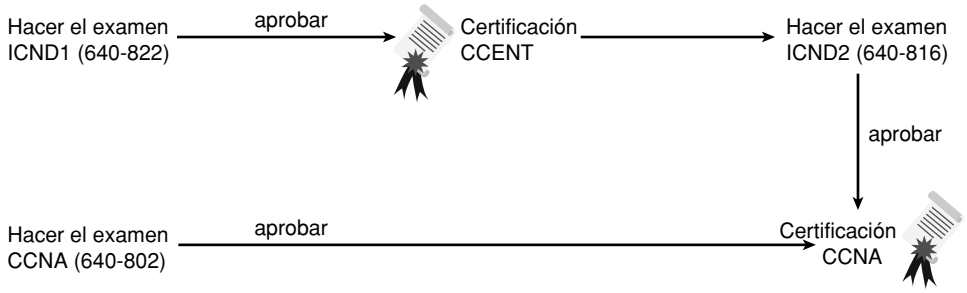


Figura I.1. Exámenes y certificaciones de Cisco para el nivel de entrada.

Como puede verse en la figura, la certificación CCENT está disponible a través del examen ICND1; no es preciso tener la certificación CCENT para obtener la certificación CCNA, sino que se puede optar por acudir directamente al examen CCNA y evitar la certificación CCENT.

Los exámenes ICND1 e ICND2 abarcan distintos conjuntos de temas, con pequeño grado de solapamiento. Por ejemplo, ICND1 trata el direccionamiento IP y la creación de subredes, mientras que ICND2 abarca una utilización más compleja de las subredes denominada Máscara de subred de longitud variable (VLSM), así que ICND2 tiene que tratar las subredes hasta cierto punto. El examen CCNA abarca todos los temas que se tratan tanto en el examen ICND1 como en el ICND2.

Aunque la popularidad de la certificación CCENT no se apreciará mientras no transcurran algunos años, la certificación CCNA de Cisco disfruta de una posición como programa de certificación más popular en el nivel de entrada. La certificación CCNA demuestra que se dispone de sólidos conocimientos sobre los componentes más importantes de la línea de productos de Cisco, a saber, routers y switches. Además demuestra que se tienen amplios conocimientos de protocolos y de las tecnologías de red.

Formato de los exámenes CCNA

Los exámenes ICND1, ICND2 y CCNA siguen un mismo formato general. Cuando se llega al centro de evaluación y se hace el registro, el encargado proporciona unas instrucciones

generales y lleva al examinado a una habitación tranquila con un PC. Una vez sentados delante del mismo, hay que hacer unas cuantas cosas antes de que empiece a contar el tiempo para el examen. Por ejemplo, se puede hacer un ejemplo de examen, para acostumbrarse al PC y al mecanismo de evaluación. Cualquier persona que tenga unos conocimientos a nivel de usuario para moverse por un PC no debe tener problemas con el entorno de evaluación.

Cuando comience el examen se le formularán unas cuantas preguntas. Primero se responde a una cuestión y después se pasa a la cuestión siguiente. *El mecanismo de examen no permite volver atrás y cambiar las respuestas.* Así es: cuando se pasa a la pregunta siguiente, la anterior no admite cambios.

Las cuestiones del examen pueden adoptar uno de los formatos siguientes:

- Respuesta múltiple (MC).
- Pequeña prueba (*test let*).
- Arrastrar y soltar (DND).
- Laboratorio simulado (*Sim*).
- Pequeña simulación (*Simlet*).

Los tres primeros tipos de cuestiones son relativamente frecuentes en muchos entornos de evaluación. El formato de respuesta múltiple sólo requiere señalar y hacer clic en un círculo situado junto a la respuesta o respuestas correctas. Tradicionalmente, Cisco indica cuántas respuestas hay que seleccionar, y el software de evaluación impide marcar un número excesivo de respuestas. Las pequeñas pruebas son cuestiones con un escenario general, con múltiples cuestiones de respuesta múltiple relativas a todo el escenario. Las cuestiones de arrastrar y soltar requieren hacer clic y mantener pulsado el botón del ratón, desplazar un botón o icono a otra zona, y soltar el botón del ratón para ubicar ese objeto en algún otro lugar; normalmente, en una lista. Por tanto, para algunas cuestiones, si se quiere conseguir una respuesta correcta es preciso poner una lista de cinco cosas en el orden correcto.

Los dos últimos tipos utilizan ambos un simulador de redes para hacer preguntas. Curiosamente, los dos tipos permiten a Cisco estimar dos capacidades muy distintas. En primer lugar, las cuestiones de tipo Sim suelen describir un problema, y nuestra tarea consiste en configura uno o más routers y switches para corregir el problema. Entonces el examen califica la pregunta basándose en la configuración que se ha modificado o añadido. Curiosamente, las cuestiones *Sim* son las únicas en las que Cisco (hasta el momento) ha confirmado abiertamente que otorga una puntuación parcial.

Las cuestiones *Simlet* son posiblemente el tipo de cuestión más difícil del examen. Estas cuestiones también hacen uso de un simulador de redes, pero en lugar de responder a la cuestión cambiando la configuración, la pregunta incluye una o más cuestiones de múltiples respuestas. Las cuestiones requieren utilizar el simulador para examinar el comportamiento actual de una red, interpretando el resultado de los posibles comandos `show` que se puedan recordar para responder a la pregunta. Las cuestiones de tipo *Sim* requieren resolver problemas relacionados con una configuración, y las *Simlets* requieren tanto analizar redes operativas como redes con problemas, relacionando los resultados de comandos `show` con nuestro conocimiento de la teoría de redes y de los comandos de configuración.

¿Cómo son los exámenes de CCNA?

Desde que estaba en primaria, siempre que el profesor anunciaba que había un examen próximamente, alguien preguntaba "¿Cómo es el examen?" Incluso en la universidad, intentábamos obtener más información sobre lo que entraría en los exámenes. En realidad, el objetivo es saber qué hay que estudiar detalladamente, qué hay que estudiar someramente, y qué es lo que no hay que estudiar.

Cisco desea ciertamente que el público conozca la gama de temas, y también que tenga una idea de las clases de conocimientos y de capacidades que se requieren para cada tema, y esto para todos los exámenes de certificación de Cisco. Con este fin, Cisco publica un conjunto de objetivos para cada examen. Los objetivos son una lista de temas concretos, como el direccionamiento IP, RIP y las VLAN. Los objetivos también implican las clases de capacidades que se precisan para el tema. Por ejemplo, un objetivo puede empezar como "Describir..." y otro podría empezar por "Describir, configurar y resolver problemas de...." El segundo objetivo indica claramente que es necesaria una comprensión profunda y exhaustiva del tema. Al enumerar los temas y el nivel de capacidad requerido, Cisco nos ayuda a prepararnos para sus exámenes.

Aunque los objetivos de los exámenes sirven de ayuda, tenga en cuenta que Cisco añade una renuncia que indica que los temas de examen que se muestran para todos los exámenes no son otra cosa que *líneas generales*. Cisco se esfuerza por mantener las cuestiones de los exámenes dentro de los límites de los objetivos de examen indicados, y ciertamente las conversaciones mantenidas con quienes están implicados muestran que todas las preguntas se analizan para determinar si se hallan o no dentro de los temas de examen marcados.

Temas del examen ICND1

La Tabla I.1 muestra los temas de examen correspondientes al examen ICND1, y los temas del examen ICND2 se muestran a continuación en la Tabla I.2. Aunque los temas de examen mostrados no están numerados en Cisco.com, Cisco Press sí numera los temas de examen para facilitar la referencia. La tabla también muestra en qué partes del libro se trata cada uno de los temas de examen. Como estos temas pueden ir cambiando con el tiempo, no deje de comprobar los temas de examen tal como aparecen en Cisco.com (específicamente, en http://www.cisco.com/go/ccna). Si realmente Cisco añadiera temas de examen en una fecha posterior, obsérvese que en el Apéndice C del libro se describe la forma de acceder a http://www.ciscopress.com y descargar información adicional sobre los nuevos temas añadidos.

Nota

La tabla incluye marcas en gris que se explicarán en la sección siguiente, "Temas del examen CCNA"

Tabla I.1. Temas del examen ICND1.

Número de referencia	Parte(s) del libro ICND1 en que se trata el tema	Tema de examen
		Describir el funcionamiento de las redes de datos
1	I	Describir el propósito y funcionamiento de distintos dispositivos de red.
2	I	Seleccionar los componentes requeridos para satisfacer una determinada especificación de red.
3	I, II, III	Utilizar los modelos ISO y TCP/IP y sus protocolos asociados para explicar la forma en que fluyen los datos a través de una red.
4	I	Describir aplicaciones comunes de las redes, incluyendo las aplicaciones para la Web.
5	I	Describir el propósito y funcionamiento básicos de los protocolos que hay en los modelos ISO y TCP.
6	I	Describir el impacto que tienen las aplicaciones sobre las redes (Voz sobre IP y Vídeo sobre IP).
7	I–IV	Interpretar los diagramas de red.
8	I–IV	Determinar la ruta que media entre dos computadoras a través de una red.
9	I, III, IV	Describir los componentes necesarios para las comunicaciones de red y de Internet.
10	I–IV	Identificar y corregir problemas de red comunes en las Capas 1, 2, 3 y 7, empleando un método basado en un modelo de capas.
11	II, III	Distinguir entre el funcionamiento de LAN/WAN y sus características.
		Implementar una pequeña red conmutada
12	II	Seleccionar los medios, cables, puertos, conectores y medios necesarios para conectar switches a otros dispositivos y computadoras de la red.
13	II	Explicar la tecnología y el método de control de acceso para las tecnologías de Ethernet.
14	II	Explicar la segmentación de redes y los conceptos básicos de gestión del tráfico.
15	II	Explicar el funcionamiento de los switches de Cisco y los conceptos básicos de conmutación.
16	II	Realizar, guardar y verificar las tareas iniciales de configuración de un switch, incluyendo la gestión de acceso remoto.
17	II	Verificar el estado de la red y el funcionamiento del switch empleando utilidades básicas (entre las que se cuentan ping, traceroute, telnet, SSH, arp, ipconfig), y comandos SHOW y DEBUG.

Tabla I.1. Temas del examen ICND1 *(continuación).*

Número de referencia	Parte(s) del libro ICND1 en que se trata el tema	Tema de examen
18	II	Implementar y verificar una seguridad básica para un switch (seguridad de puertos, desactivar los puertos).
19	II	Identificar, prescribir y resolver problemas comunes en medios de redes conmutadas, problemas de configuración, autonegociación y fallos de hardware en el switch.
		Implementar un esquema de direccionamiento IP y de servicios IP para satisfacer los requisitos de red de una pequeña sucursal
20	I, III	Describir la necesidad y el papel del direccionamiento en una red.
21	I, III	Crear y aplicar un esquema de direccionamiento en una red.
22	III	Asignar y verificar direcciones IP válidas a computadoras, servidores y dispositivos de red en un entorno LAN.
23	IV	Explicar las utilidades y funcionamiento básico de NAT en una pequeña red conectada a un solo ISP.
24	I, III	Describir y verificar el funcionamiento de DNS.
25	III, IV	Describir el funcionamiento y los beneficios de utilizar el direccionamiento IP público y privado.
26	III, IV	Habilitar NAT para una pequeña red que tenga una sola conexión a un único ISP empleando SDM, y verificar su funcionamiento empleando CLI y ping.
27	III	Configurar, verificar y resolver problemas de funcionamiento de DHCP y de DNS en un router (incluyendo: CLI/SDM).
28	III	Implementar servidores de direccionamiento estático y dinámico para las computadoras de un entorno LAN.
29	III	Identificar y corregir problemas de direccionamiento IP.
		Implementar una pequeña red enrutada
30	I, III	Describir los conceptos básicos de enrutamiento (incluyendo el reenvío de paquetes, y el proceso de búsqueda de routers).
31	III	Describir el funcionamiento de los routers de Cisco (incluyendo el proceso de arranque del router, POST, y los componentes del router).
32	I, III	Seleccionar los medios adecuados, cables, puertos y conectores necesarios para conectar routers a otros dispositivos y computadoras de la red.
33	III	Configurar, verificar y resolver problemas de RIPv2.
34	III	Acceder a la CLI del router y emplearla para configurar los parámetros básicos.

Tabla I.1. Temas del examen ICND1 *(continuación).*

Número de referencia	Parte(s) del libro ICND1 en que se trata el tema	Tema de examen
35	III	Conectar, configurar y verificar el estado de funcionamiento de la interfaz de un dispositivo.
36	III	Verificar la configuración y conectividad de red de un dispositivo empleando ping, traceroute, telnet, SSH u otras utilidades.
37	III	Realizar y verificar tareas de configuración de enrutamiento para una ruta estática o predeterminada recibiendo unos requisitos específicos de enrutamiento.
38	III	Administrar los archivos de configuración del IOS (incluyendo guardar, editar, actualizar, restaurar).
39	III	Administrar el IOS de Cisco.
40	III	Implementar la seguridad física y una contraseña.
41	III	Verificar el estado de la red y el funcionamiento del router empleando utilidades básicas (incluyendo ping, traceroute, telnet, SSH, arp, ipconfig) y también comandos SHOW y DEBUG.
		Explicar y seleccionar las tareas administrativas adecuadas que se requieren para una WLAN
42	II	Describir los estándares asociados a los medios inalámbricos (incluyendo IEEE, WI-FI Alliance, ITU/FCC).
43	II	Identificar y describir el propósito de los componentes de una pequeña red inalámbrica (incluyendo SSID, BSS, ESS).
44	II	Identificar los parámetros básicos necesarios para configurar una red inalámbrica para asegurarse de que los dispositivos se conectan al punto de acceso correcto.
45	II	Comparar y contrastar las características de seguridad inalámbrica y las capacidades de la seguridad WPA (incluyendo open, WEP, WPA-1/2).
46	II	Identificar problemas comunes en la implementación de redes inalámbricas.
		Identificar las amenazas a la seguridad de una red y describir los métodos generales para mitigar esas amenazas
47	I	Explicar las crecientes amenazas actuales contra la seguridad de las redes y la necesidad de implementar una política exhaustiva de seguridad para mitigar esas amenazas.
48	I	Explicar métodos generales para mitigar amenazas comunes de seguridad en dispositivos de red, computadoras y aplicaciones.

Tabla I.1. Temas del examen ICND1 *(continuación)*.

Número de referencia	Parte(s) del libro ICND1 en que se trata el tema	Tema de examen
49	I	Describir las funciones de los dispositivos y aplicaciones comunes de seguridad.
50	I, II, III	Describir las prácticas de seguridad recomendables, incluyendo los pasos iniciales para garantizar la seguridad de los dispositivos de red.
		Implementar y verificar enlaces WAN
51	IV	Describir distintos métodos para conectarse a una WAN.
52	IV	Configurar y verificar una conexión serie WAN básica.

Temas del examen ICND2

La Tabla I.2 muestra los temas de examen correspondientes al examen ICND2 (640-816), junto con las partes de este libro en que se trata cada tema.

Tabla I.2. Temas del examen ICND2.

Número de referencia	Parte(s) del libro ICND2 en que se trata el tema	Tema de examen
		Configurar, verificar y resolver problemas de un switch con comunicaciones entre switches y VLANs
101	I	Describir las tecnologías mejoradas de conmutación (incluyendo VTP, RSTP, VLAN, PVSTP, 802.1q).
102	I	Describir la forma en que las VLAN crean redes separadas lógicamente y la necesidad de un enrutamiento entre ellas.
103	I	Configurar, verificar y resolver problemas de VLANs.
104	I	Configurar, verificar y resolver problemas de *trunking* en switches de Cisco.
105	II	Configurar, verificar y resolver problemas de enrutamiento entre VLANs.
106	I	Configurar, verificar y resolver problemas de VTP.
107	I	Configurar, verificar y resolver problemas relacionados con el funcionamiento de RSTP.

Tabla I.2. Temas del examen ICND2 *(continuación).*

Número de referencia	Parte(s) del libro ICND1 en que se trata el tema	Tema de examen
108	I	Interpretar el resultado de distintos comandos show y debug para verificar el estado operacional de una red conmutada de Cisco.
109	I	Implementar una seguridad básica en el switch (incluyendo seguridad de puertos, puertos sin asignar, acceso troncal, etc.).
		Implementar un esquema de direccionamiento IP y de servicios IP adecuado para satisfacer los requisitos de red de una sucursal de una empresa de tamaño medio
110	II	Calcular y aplicar a una red un diseño de direccionamientos IP VLSM.
111	II	Determinar el esquema de direccionamiento sin clase adecuado para utilizar VLSM y resúmenes para satisfacer los requisitos de direccionamiento de un entorno LAN/WAN.
112	V	Describir los requisitos tecnológicos necesarios para ejecutar IPv6 (incluyendo los protocolos, pilas duales, túneles etc.).
113	V	Describir las direcciones IPv6.
114	II, III	Identificar y corregir problemas comunes asociados al direccionamiento IP y a las configuraciones de las computadoras.
		Configurar y resolver problemas de funcionamiento básico y de enrutamiento en dispositivos de Cisco
115	III	Comparar y contrastar métodos de enrutamiento y protocolos de enrutamiento.
116	III	Configurar, verificar y resolver problemas de OSPF.
117	III	Configurar, verificar y resolver problemas de EIGRP.
118	II, III	Verificar la configuración y la conectividad empleando ping, traceroute y telnet o SSH.
119	II, III	Resolver problemas de implementación del enrutamiento.
120	II, III, IV	Verificar el funcionamiento del hardware y del software de un router empleando comandos SHOW y DEBUG.
121	II	Implementar una seguridad básica para los puertos del router.
		Implementar, verificar y resolver problemas de NAT y de ACL en la red de una sucursal de una empresa de tamaño medio
122	II	Describir el propósito y los tipos de listas de control de acceso.
123	II	Configurar y aplicar listas de control de acceso basadas en requisitos de filtrado de la red.

Tabla I.2. Temas del examen ICND2 *(continuación).*

Número de referencia	Parte(s) del libro ICND2 en que se trata el tema	Tema de examen
124	II	Configurar y aplicar una lista de control de acceso para limitar el acceso al router vía telnet y SSH.
125	II	Verificar y monitorizar las ACLs en un entorno de red.
126	II	Resolver problemas de implementación de las ACLs.
127	V	Explicar el funcionamiento básico de NAT.
128	V	Configurar la Conversión de direcciones de red para unos requisitos de red dados empleando la CLI.
129	V	Resolver problemas de implementación de NAT.
		Implementar y verificar enlaces WAN
130	IV	Configurar y verificar Frame Relay en un router de Cisco.
131	IV	Resolver problemas de implementación de WAN.
132	IV	Describir la tecnología VPN (incluyendo su importancia, beneficios, rol, impacto y componentes).
133	IV	Configurar y verificar una conexión PPP entre routers de Cisco.

Temas del examen CCNA

En la versión previa de los exámenes, el examen CCNA abarcaba gran parte de lo que está en el examen ICND (640-811), y además abarcaba algunos temas del examen INTRO (640-821). El nuevo examen CCNA (640-802) abarca todos los temas que hay tanto en el examen ICND1 (640-822) como en el examen ICND2 (640-816). Una de las razones por las que hay un tratamiento más equilibrado en los exámenes es que algunos de los temas que estaban antes en el segundo examen han pasado ahora al primero.

El nuevo examen CCNA (640-802) trata todos los temas abarcados por los exámenes ICND1 e ICND2. Los temas oficiales del examen CCNA 640-802, que están publicados en http://www.cisco.com, incluyen todos los temas enumerados en la Tabla I.2 para el examen ICND2, así como la mayoría de los temas de examen correspondientes al examen ICND1 que se muestran en la Tabla I.1. Los únicos temas de examen para estas dos tablas que no se enumeran como temas de examen para CCNA son los temas que se han marcado en gris en la Tabla I.1. Sin embargo, obsérvese que los temas en gris se tratan en el examen CCNA 640-802. Estos temas no se muestran entre los temas de examen de CCNA porque uno de los temas de examen de ICND2 se refiere precisamente a los mismos conceptos.

Contenidos del curso ICND1 e ICND2

Otra forma de hacerse a la idea de los temas que aparecen en los exámenes consiste en examinar los contenidos de los cursos relacionados. Cisco ofrece dos cursos autorizados que están relacionados con CCNA: *Interconnecting Cisco Network Devices 1* (ICND1) e *Interconnecting Cisco Network Devices 2* (ICND2). Cisco autoriza a los *Certified Learning Solutions Providers* (CLSP) y a los *Certified Learning Partners* (CLP) para que impartan esas clases. Estas compañías autorizadas también pueden crear libros de curso personalizados y exclusivos que hagan uso de este material; en ciertos casos sirven para impartir clases orientadas a superar el examen CCNA.

Acerca de las Guías oficiales para los exámenes de certificación CCENT/CCNA ICND1 y CCNA ICND2

Según se ha indicado anteriormente, Cisco ha separado el contenido abarcado por el examen CCNA en dos partes: temas que típicamente emplean los ingenieros que trabajan en redes de empresas de pequeño tamaño (ICND1), y los temas adicionales, que normalmente emplean los ingenieros en empresas de tamaño medio, se tratan en el examen ICND2. De forma similar, la serie de Cisco Press llamada CCNA Exam Certification Guide contiene dos libros para CCNA: *CCENT/CCNA ICND1 Guía Oficial para el examen de Certificación* y *CCNA ICND2 Guía Oficial para el examen de Certificación*. Estos dos libros tratan toda la gama de temas de ambos exámenes, típicamente con algo más de profundidad que la exigida en los exámenes, para garantizar que los libros sirvan de preparación para las preguntas más difíciles del examen.

Las secciones siguientes enumeran la gama de temas que se tratan en este libro y en el libro *CCENT/CCNA ICND1 Guía Oficial para el examen de Certificación*. Ambos libros tienen las mismas características básicas, así que si va a leer este libro y el libro de ICND1, no necesita leer la introducción de los dos. Además, para quienes utilicen ambos libros para prepararse para el examen de CCNA 640-802 (en lugar de optar por la posibilidad de hacer dos exámenes), al final de esta introducción se muestra una sugerencia de plan de lectura.

Objetivos y métodos

El objetivo más importante, y quizá el más evidente de este libro, es ayudar al lector a pasar el examen ICND2 o el examen CCNA. De hecho, si el objetivo primario de este libro fuera otro, su título induciría a confusión. Sin embargo, los métodos que se emplean en este libro para ayudarle a pasar los exámenes también están diseñados para hacer que sepa mucho más sobre la forma de llevar a cabo sus tareas.

Este libro utiliza varias tecnologías clave para ayudarle a descubrir los temas de examen respecto a los cuales necesita repasar más, para ayudarle a entender por completo y a recordar los detalles, y para ayudarle a demostrarse a sí mismo que ha afianzado sus conocimientos sobre esos temas. Por tanto, este libro no intenta ayudarle a pasar los exámenes sólo por memorización, sino mediante un verdadero aprendizaje y comprensión de los temas. La certificación CCNA es la base de muchas certificaciones profesionales de Cisco, y le haríamos un flaco servicio si este libro no le ayudase a aprender realmente el temario. Por tanto, el libro le ayudará a pasar el examen CCNA empleando los métodos siguientes:

- Ayudándole a descubrir los temas del examen que todavía no domina.
- Proporcionándole explicaciones e información para llenar lagunas en sus conocimientos.
- Aportando ejercicios que mejoran su capacidad para recordar y deducir las respuestas de las preguntas del examen.

Características del libro

Para ayudarle a personalizar su forma de estudiar empleando estos libros, los capítulos principales tienen varias características que le ayudarán a aprovechar el tiempo del mejor modo posible:

- **Cuestionario "Ponga a prueba sus conocimientos".** Cada capítulo comienza con un cuestionario que le ayudará a determinar la cantidad de tiempo que necesita invertir para estudiar el capítulo.
- **Temas fundamentales.** Son las secciones principales de cada capítulo. Explican los protocolos, los conceptos y la configuración para los temas del capítulo.
- **Ejercicios para la preparación del examen.** Al final de la sección "Temas fundamentales" de los capítulos, la sección "Ejercicios para la preparación del examen" muestra una lista de actividades de estudio que debería realizarse al final del capítulo. Cada capítulo incluye las actividades que tienen más sentido para estudiar los temas de ese capítulo. Las actividades incluyen lo siguiente:
  - **Repaso de los temas clave.** El icono "Tema clave" se muestra junto a los elementos más importantes de la sección "Temas fundamentales" del capítulo. La actividad "Repaso de los temas clave" muestra los temas clave del capítulo, y su número de página. Aunque todo el contenido del capítulo podría aparecer en el examen, decididamente es preciso conocer la información mostrada en los temas clave, así que será conveniente repasarlos.
  - **Complete de memoria las tablas y las listas.** Para ayudarle a ejercitar su memoria y para memorizar ciertas listas, muchas de las listas y tablas más importantes del capítulo se incluyen en el Apéndice J del DVD. Este documento sólo contiene información parcial, y le permitirá completar la tabla o la lista. En el Apéndice K se muestran las mismas tablas y listas, pero completas, para facilitar las comparaciones.

  - **Definición de los términos clave.** Aunque es improbable que en los exámenes aparezca algo así como "Definir este término", los exámenes de CCNA requieren ciertamente aprender y conocer mucha terminología de redes. Esta sección muestra los términos más importantes del capítulo, y le pide que escriba una breve definición y que compare su respuesta con el glosario que hay al final del libro.
  - **Referencias de comandos.** Algunos capítulos del libro abarcan una gran cantidad de comandos EXEC de configuración. Estas listas muestran los comandos presentados en el capítulo, junto con una explicación. Para preparar el examen, utilícelas como referencia, pero lea también las tablas una vez cuando haga los "Ejercicios para la preparación del examen", para asegurarse de que recuerda lo que hacen todos los comandos.
- **Vídeos de subredes.** El DVD asociado contiene una serie de vídeos que muestran la forma de calcular distintos datos relativos al direccionamiento IP y a las subredes; en particular, empleando los métodos abreviados que se describen en este libro.
- **Prácticas de subredes.** El Apéndice D del DVD contiene un gran grupo de problemas de prácticas de subredes, con las respuestas y explicaciones de la forma en que se han obtenido las respuestas. Es un excelente recurso para prepararse para crear subredes de forma rápida y correcta.
- **Escenarios de prácticas basados en el DVD.** El Apéndice F del DVD contiene varios escenarios de redes para realizar un estudio adicional. Estos escenarios describen varias redes con distintos requisitos, y conducen al lector a través del diseño conceptual, la configuración y la verificación. Estos escenarios son útiles para mejorar nuestras capacidades prácticas, aun cuando no se disponga de un equipo de laboratorio.
- **Sitio web asociado.** El sitio web http://www.ciscopress.com/title/1587201828 publica materiales totalmente actualizados que clarifican aún más los temas de examen más complejos. Visite regularmente este sitio para obtener publicaciones nuevas y actualizadas escritas por el autor, que le ofrecerán perspectivas adicionales de los temas más problemáticos del examen.

Cómo está organizado este libro

El libro contiene 18 capítulos principales: los Capítulos del 1 al 17, además del Capítulo 18, que contiene material de resumen y sugerencias relativas a la forma de abordar los exámenes. Cada capítulo principal abarca un subconjunto de los temas del examen ICND2. Los capítulos principales están organizados en secciones, y abarcan los temas siguientes:

- Parte I: Conmutación de redes
  - **Capítulo 1, "LANs virtuales"**. Este capítulo explica los conceptos y configuración relacionados con las LAN virtuales, incluyendo el *trunking* VLAN y el Protocolo de *trunking* VLAN.

- **Capítulo 2, "Protocolo de árbol de extensión"**. Este capítulo estudia profundamente los conceptos que subyacen al Protocolo de árbol de extensión original (STP), y también al nuevo Rapid STP (RSTP), incluyendo los conceptos, la configuración y la resolución de problemas.
- **Capítulo 3, "Resolución de problemas con la conmutación LAN"**. Este capítulo explica ideas generales relativas a la forma de resolver problemas de red, y la mayor parte del capítulo se centra en el proceso de reenvío que utilizan los switches LAN.

• Parte II: Enrutamiento IP
  - **Capítulo 4, "Enrutamiento IP: rutas estáticas y conectadas"**. Este capítulo examina la forma en que los routers añaden tanto rutas estáticas como conectadas a la tabla de enrutamiento, y además revisa los conceptos que subyacen a la forma en que los routers enrutan o reenvían los paquetes.
  - **Capítulo 5, "VLSM y resumen de rutas"**. Este capítulo explica la forma en que el enrutamiento IP y los protocolos de enrutamiento pueden soportar el uso de distintas máscaras de subred en una sola red con clase (VLSM), así como los conceptos matemáticos que subyacen a la forma en que los routers pueden resumir múltiples rutas en una sola entrada de la tabla de enrutamiento.
  - **Capítulo 6, "Listas de control de acceso IP"**. Este capítulo examina la forma en que las ACL pueden filtrar paquetes de tal modo que el router no reenvía ciertos paquetes. El capítulo examina los conceptos y la configuración de las ACL estándar y extendidas, incluyendo las ACL numeradas y con nombre.
  - **Capítulo 7, "Resolución de problemas de enrutamiento IP"**. Este capítulo muestra un plan estructurado relativo a la forma de aislar problemas relacionados con dos computadoras que deberían ser capaces de enviarse paquetes entre sí, pero no pueden. El capítulo incluye también unos cuantos consejos y herramientas, que sirven de ayuda para atacar los problemas de enrutamiento.

• Parte III: Configuración y resolución de problemas con los protocolos de enrutamiento
  - **Capítulo 8, "Teoría de los protocolos de enrutamiento"**. Este capítulo explica la teoría que subyace a los protocolos por vector de distancia y de estado del enlace.
  - **Capítulo 9, "OSPF"**. Este capítulo examina OSPF, incluyendo más detalles relativos a la teoría del estado del enlace tal como se implementa en OSPF, y de la configuración de OSPF.
  - **Capítulo 10, "EIGRP"**. Este capítulo examina EIGRP, incluyendo una descripción de la teoría que subyace a EIGRP, así como la configuración y verificación de EIGRP.
  - **Capítulo 11, "Resolución de problemas en los protocolos de enrutamiento"**. Este capítulo explica algunas de las razones típicas por las cuales los protocolos de enrutamiento no consiguen intercambiar información de enrutamiento, y muestra ejemplos específicos de problemas comunes tanto en OSPF como en EIGRP.

- Parte IV: Redes de área amplia
  - **Capítulo 12, "WANs punto a punto"**. Este breve capítulo revisa los conceptos básicos de las WANs y examina con más detalle PPP, incluyendo CHAP.
  - **Capítulo 13, "Conceptos de Frame Relay"**. Este capítulo se centra en la terminología y teoría que subyace al protocolo Frame Relay, incluyendo las opciones de direccionamiento IP cuando se utiliza Frame Relay.
  - **Capítulo 14, "Configuración y resolución de problemas en Frame Relay"**. Este capítulo muestra toda una gama de opciones de configuración para Frame Relay, incluyendo las subinterfaces punto a punto y multipunto. También explica la mejor manera de utilizar el comando `show` para aislar la causa inicial de problemas comunes de Frame Relay.
  - **Capítulo 15, "Redes privadas virtuales"**. Este capítulo examina los conceptos y protocolos que se utilizan para hacer seguras las VPNs a través de Internet. El capítulo incluye los fundamentos de IPsec.
- Parte V: Escalado del espacio de direcciones IP
  - **Capítulo 16, "Conversión de direcciones de red"**. Este capítulo examina detalladamente los conceptos que subyacen al agotamiento del espacio de direcciones IPv4, y la forma en que NAT, y en particular la opción de Conversión de direcciones de puerto (PAT) ayuda a resolver el problema. El capítulo muestra también la forma de configurar NAT en routers que hacen uso de la CLI del IOS.
  - **Capítulo 17, "IP Versión 6"**. Este capítulo presenta las bases de IPv6, incluyendo el formado de direcciones de 128 bits, el soporte de OSPF y de EIGRP para IPv6, y la configuración nativa básica de IPv6. También presenta el concepto de *tunneling* IPv6 y las estrategias de migración.
- Parte VI: Preparación final
  - **Capítulo 18, "Preparación Final"**. Este capítulo sugiere un plan para la preparación final una vez terminadas las partes principales del libro, y en particular explica las muchas opciones de estudio que están disponibles en el libro.
- Parte VII: Apéndices (impresos)
  - **Apéndice A, "Respuestas de los cuestionarios 'Ponga a prueba sus conocimientos'"**. Incluye respuestas para todas las cuestiones de los Capítulos del 1 al 17.
  - **Apéndice B, "Tabla de conversión de decimal a binario"**. Muestra los valores decimales del 0 al 255, junto con sus equivalentes en binario.
  - **Apéndice C, "Actualizaciones del examen ICND2: Versión 1.0"**. Este apéndice abarca toda una gama de temas breves que aclaran o amplían temas tratados anteriormente en el libro. El apéndice se actualiza de vez en cuando y se publica en `http://www.ciscopress.com/ccna`, incluyéndose la versión más reciente disponible en el momento de efectuar la impresión como Apéndice C. (La primera página del apéndice contiene instrucciones relativas a la forma de comprobar si hay una versión más reciente del Apéndice C disponible en la Web.)

— **Glosario**. El glosario contiene definiciones de todos los términos que aparecen en la sección "Definiciones de los términos clave" que aparece al final de los Capítulos del 1 al 17.

- Parte VIII: Apéndices (en el DVD)

Los apéndices siguientes están disponibles en formato PDF en el DVD que acompaña al libro:

— **Apéndice D, "Subnetting Practice" (prácticas de subredes)**. Aunque no se tratan en los capítulos impresos del libro, las subredes son posiblemente la más importante de las capacidades que se asumen como requisito previo para el examen ICND2. Este apéndice, así como los Apéndices E, H e I, incluyen materiales de la *Guía Oficial para el examen de Certificación* **CCENT/CCNA ICND1** para quienes hayan comprado este libro pero no el libro de ICND1. En particular, este apéndice incluye un gran número de problemas prácticos de subredes, y se muestran las respuestas. Las respuestas utilizan tanto procesos binarios como procesos decimales abreviados, que se describen en el Capítulo 12 del libro de ICND1; el Apéndice H de este libro es un duplicado del Capítulo 12 del libro de ICND1.

— **Apéndice E, "Subnetting Reference Pages" (páginas de referencia de subredes)**. Este apéndice resume el proceso necesario para hallar la respuesta a varias cuestiones clave sobre subredes, mostrando los detalles en una sola página. El objetivo es proporcionar una referencia cómoda a la que sea posible hacer referencia cuando se hacen prácticas con subredes.

— **Apéndice F, "Additional Scenarios" (escenarios adicionales)**. Un método para mejorar nuestras capacidades de análisis de redes y de resolución de problemas consiste en examinar tantos escenarios distintos de red como sea posible, para después recibir una realimentación relativa a si hemos llegado o no a las respuestas correctas. Este apéndice ofrece varios de estos escenarios.

— **Apéndice G, "Video Scenario Reference" (referencia del escenario de vídeo)**. El DVD incluye varios vídeos de subredes que muestran la forma de utilizar los procesos tratados en el Apéndice H (que está copiado del Capítulo 12 del libro de ICND1). Este apéndice contiene copias de los elementos clave de esos vídeos, lo cual puede ser útil cuando se vean los vídeos (para que no sea preciso estar avanzando y retrocediendo en el vídeo).

— **Apéndice H, "ICND1 Chapter 12: IP Addressing and Subnetting" (Capítulo 12 de ICND1. Direccionamiento IP y *subnetting* IP)**. Este apéndice es un duplicado del Capítulo 12 del libro **CCENT/CCNA ICND1**: este capítulo explica el direccionamiento IP y las subredes, que se consideran un conocimiento previo indispensable para el examen de ICND2. El Apéndice H se incluye en el libro para quienes no dispongan de una copia del libro **CCENT/CCNA ICND1**, pero necesiten revisar y aprender más sobre las subredes.

— **Apéndice I, "ICND1 Chapter 17: WAN Configuration" (Capítulo 17 de ICND1: Configuración WAN)**. Este apéndice es un duplicado del Capítulo 17 del libro **CCENT/CCNA ICND1**. El Capítulo 12 de este libro (ICND2), "WANs

punto a punto", hace la sugerencia consistente en revisar unas cuantas cuestiones previas, que se muestran en este capítulo. El capítulo se incluye en el libro para quienes no tengan una copia del libro **CCENT/CCNA ICND1**.

— **Apéndice J, "Memory Tables" (Tablas de memoria)**. Este apéndice contiene las tablas clave y las listas de todos los capítulos, descartando parte del contenido. Puede imprimir el apéndice y, como ejercicio de memoria, completar las tablas y las listas. El objetivo es ayudarle a memorizar hechos que pueden serle de utilidad en los exámenes.

— **Apéndice K, "Answer Key to the Memory Tables" (Clave de respuesta para las tablas de memoria)**. Este Apéndice contiene la clave de respuesta para los ejercicios del Apéndice J.

— **Apéndice L, "ICND2 Open-Ended Questions" (preguntas de respuesta abierta ICNDZ)**. Este apéndice es una herencia de ediciones anteriores del libro. Las ediciones anteriores tenían preguntas abiertas con el propósito de que sirvieran de ayuda para estudiar el examen, pero las características nuevas hacen innecesarias estas cuestiones. Por comodidad, las viejas preguntas se incluyen aquí, sin modificaciones respecto a la última edición.

Forma de utilizar este libro para preparar el examen ICND2 (640-816)

Este libro se ha diseñado con dos objetivos primordiales: ayudar al lector a estudiar para el examen ICND2 y ayudarle a estudiar para el examen CCNA empleando tanto este libro como la Guía **CCENT/ CCNA ICND1**. Es fácil utilizar este libro para preparar el examen ICND2: lea los capítulos uno tras otro, y siga las sugerencias de estudio que hay en el Capítulo 18.

Para los capítulos principales de este libro (los capítulos del 1 al 17) se tiene una cierta holgura en lo tocante a qué proporción del capítulo es preciso leer. En algunos casos, quizá se conozca ya gran parte de la información tratada en el capítulo. Para ayudarle a decidir cuánto tiempo va a invertir en cada capítulo, éste comienza por un examen del tipo "Ponga a prueba sus conocimientos". Si responde correctamente a todas las preguntas, o si sólo falla una de ellas, quizá quiera pasar al final del capítulo, y hacer los "Ejercicios para la preparación del examen". La Figura I.2 muestra la estructura general.

Cuando haya terminado los Capítulos del 1 al 17, puede utilizar las líneas generales que se muestran en el Capítulo 18 para organizar el resto de las tareas de preparación del examen. Ese capítulo incluye las siguientes sugerencias:

- Busque en http://www.ciscopress.com la versión más reciente del Apéndice C, que puede incluir temas adicionales para su estudio.
- Haga prácticas de subredes empleando las herramientas que están disponibles en los apéndices del DVD.

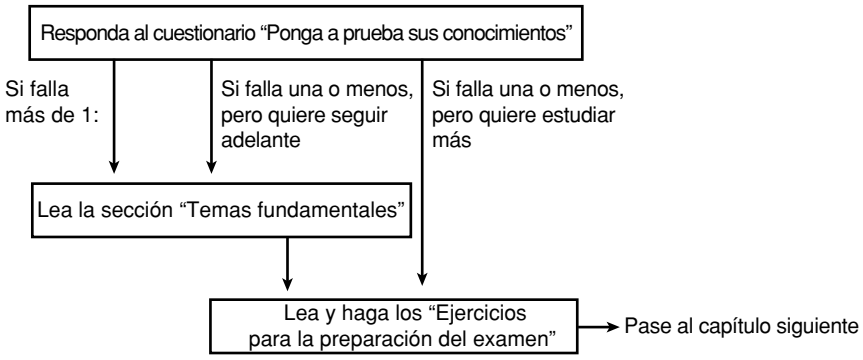


Figura I.2. Forma de enfocar los capítulos de este libro.

- Repita las tareas que hay en las secciones "Ejercicios para la preparación del examen" al final de todos los capítulos.
- Revise los escenarios que hay en el Apéndice F del DVD.
- Revise todas las cuestiones del cuestionario "Ponga a prueba sus conocimientos".

Forma de utilizar estos libros para preparar el examen CCNA 640-802

Si tiene intención de obtener la certificación CCNA empleando la opción de un solo examen, consistente en presentarse al examen CCNA 640-802, puede emplear este libro junto con el libro **CCENT/CCNA ICND1**.

Los dos libros se han diseñado para ser utilizado a la vez cuando se estudia para el examen CCNA. Se tienen dos opciones en lo tocante al orden en que se pueden leer los libros. La primera opción, y la más evidente, consiste en leer primero el libro de ICND1, y pasar después a este libro (el de ICND2). La otra opción consiste en leer todo el tratamiento de ICND1 relativo a cierto tema, y leer después el tratamiento que se hace en el libro ICND2 respecto a ese mismo tema, para después volver al ICND1. La Figura I.3 muestra la opción que se sugiere para leer ambos libros.

Las dos opciones del plan de lectura tienen sus ventajas. Al pasar de un libro a otro se puede hacer más fácil el estudio de un tema general en cada momento. Sin embargo, obsérvese que existe una cierta superposición entre ambos exámenes, así que en los libros también se hallará una cierta superposición. Tomando como base los comentarios de los lectores de ediciones anteriores de estos libros, los que eran primerizos en las redes iban generalmente mejor leyendo primero el primer libro y después el segundo, mientras que los lectores que tenían más experiencia y conocimientos, antes de empezar a leer los libros solían encontrar preferible un plan de lectura como el que se muestra en la Figura I.3.

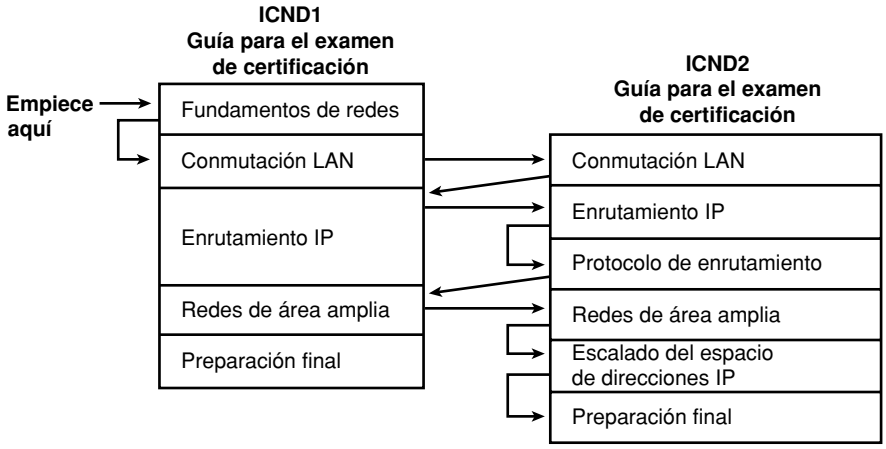


Figura I.3. Plan de lectura cuando se estudia para el examen CCNA.

Obsérvese que para la preparación final se puede utilizar el capítulo final de este libro (El Capítulo 18) en lugar del capítulo de preparación final (Capítulo 18) del libro de ICND1.

Además del flujo que se muestra en la Figura I.3, cuando se estudia para el examen CCNA (y no para los exámenes ICND1 e ICND2), es preciso dominar la creación de subredes IP antes de pasar a lo relativo al enrutamiento IP y los protocolos de enrutamiento (las partes segunda y tercera del libro). Este libro no revisa las subredes ni la aritmética subyacente en el texto impreso, y supone que ya se conoce la forma de hallar las respuestas. Esos capítulos de ICND2, especialmente el Capítulo 5, serán mucho más fáciles de entender si resulta sencillo llevar a cabo la aritmética de subredes asociada.

Para más información

Es posible que Cisco haga cambios que afecten a la certificación CCNA de vez en cuando. Siempre hay que consultar http://www.cisco.com/go/ccna para disponer de los últimos detalles.

La certificación CCNA es muy posiblemente la certificación más importante de Cisco, y es posible que la nueva certificación CCENT sobrepase a CCNA en el futuro. Ciertamente, CCNA es la certificación de Cisco más extendida y se requiere para otras certificaciones; además, es el primer paso para resaltar como persona que posee unos conocimientos probados respecto a Cisco.

Este libro se ha diseñado para que sirva de ayuda para conseguir la certificación CCNA. Este es el libro de la certificación CCNA ICND2 de la única editorial autorizada por Cisco. El personal de Cisco Press considera que este libro puede, ciertamente, servir de ayuda para obtener la certificación CCNA; sin embargo, ¡el verdadero trabajo depende del lector! Confiamos en que el tiempo que invierta le resulte rentable.

Temas* del examen ICND2 publicados por Cisco que se tratan en esta parte

Configurar, verificar y resolver problemas de un switch con las VLANs y las comunicaciones entre switches

- Describir las tecnologías mejoradas de conmutación (incluyendo: VTP, RSTP, VLAN, PVSTP, 802.1q).
- Describir la forma en que las VLAN crean redes lógicamente separadas y la necesidad de efectuar un enrutamiento entre ellas.
- Configurar, verificar y resolver problemas en las VLANs.
- Configurar, verificar y resolver problemas de *trunking* en switches de Cisco.
- Configurar, verificar y resolver problemas de VTP.
- Configurar, verificar y resolver problemas de funcionamiento de RSTP.
- Interpretar los resultados de distintos comandos show y debug para verificar el estado operacional de una red con switches de Cisco.
- Implementar una seguridad básica en el switch (incluyendo: seguridad de puertos, puertos no asignados, acceso troncal, etc.).

* No olvide consultar en http://www.cisco.com los últimos temas de examen publicados.

PARTE I

Conmutación de LANs

Capítulo 1 LANs Virtuales

Capítulo 2 Protocolo de árbol de Extensión

Capítulo 3 Resolución de problemas de conmutación LAN

Este capítulo trata los siguientes temas:

Conceptos de LANs virtuales: En esta sección se explican el significado y el propósito de las VLANs, el *trunking* VLAN, y el Protocolo de *trunking* VLAN (VTP, *VLAN Trunking Protocol*).

Configuración y verificación de VLAN y de *trunking* VLAN: Esta sección muestra cómo configurar las VLANs y los troncales en los switches catalyst de Cisco.

Configuración y verificación de VTP: En esta última sección se explica cómo configurar y solucionar problemas en las instalaciones VTP.

CAPÍTULO 1

LANs virtuales

La primera parte de este libro, que incluye los Capítulos 1, 2 y 3, se centra en el mundo de las LANs. El Capítulo 1 examina los conceptos y las configuraciones relacionados con las LANs virtuales, mientras el Capítulo 2 explica cómo el Protocolo de árbol de extensión (STP, *Spanning Tree Protocol*) previene bucles en una red con switches. Finalmente, el Capítulo 3 aúna conceptos relativos a las LAN mientras explora el proceso de resolución de los problemas comunes en las mismas.

Como se menciona en la Introducción, este libro asume que se tiene conocimientos sólidos de los temas más importantes tratados en el examen ICND1. Si no tiene claro estos prerrequisitos, puede consultarlos en la lista de conocimientos previos requeridos en este libro, bajo el título "Temas del examen ICND1" en la Introducción.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las diez preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 1.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimientos que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

Tabla 1.1. Relación entre las preguntas del cuesionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	**Preguntas**
Conceptos de LANs virtuales	1-5
Configuración y verificación de VLAN y de *trunking* VLAN	6-8
Configuración y verificación de VTP	9-10

1. En una LAN, ¿cuál de los siguientes términos es el que más se equipara al término VLAN?
   a. Dominio de colisión
   b. Dominio de difusión
   c. Dominio de subred
   d. Un solo switch
   e. Troncal.
2. Imagine un switch con tres VLANs configuradas. ¿Cuántas subredes IP se necesitan, asumiendo que todos los hosts de todas las VLANs desean utilizar TCP/IP?
   a. 0
   b. 1
   c. 2
   d. 3
   e. Con la información proporcionada no se puede contestar.
3. ¿Cuál de lo siguiente encapsula completamente la trama Ethernet original en una cabecera de *trunking* en lugar de insertar otra cabecera en la cabecera Ethernet original?
   a. VTP
   b. ISL
   c. 802.1Q
   d. Ambos, ISL y 802.1Q
   e. Ninguna respuesta es correcta.
4. ¿Cuál de lo siguiente añade la cabecera de *trunking* para todas las VLANs excepto una?
   a. VTP
   b. ISL
   c. 802.1Q
   d. Ambos, ISL y 802.1Q
   e. Ninguna respuesta es correcta.
5. ¿Cuál de los siguientes modos de VTP permite que las VLANs sean configuradas en un switch?
   a. Cliente
   b. Servidor
   c. Transparente
   d. Dinámico
   e. Ninguna respuesta es correcta.
6. Imagine que le dicen que el switch 1 está configurado con el parámetro `auto` para formar un troncal en su interfaz Fa0/5, que está conectada al switch 2. Tiene que

configurar el switch 2. ¿Cuál de los siguientes valores para formar un troncal permitirá que éste funcione?

a. Configurar el trunking a on

b. Auto

c. Desirable

d. Access

e. Ninguna respuesta es correcta.

7. Un switch acaba de llegar de Cisco. El switch no ha sido nunca configurado con ninguna VLAN, configuración de VTP, o cualquier otra configuración. Un ingeniero entra en el modo de configuración y ejecuta el comando vlan 22, seguido del comando name Hannahs-VLAN. ¿Cuáles de las siguientes respuestas son ciertas?

a. La VLAN 22 aparecerá en la salida del comando show vlan brief.

b. La VLAN 22 aparecerá en la salida del comando show running-config.

c. Este proceso no crea la VLAN 22

d. La VLAN 22 no existirá en el switch hasta que al menos se asigne una interfaz a esta VLAN.

8. ¿Cuál de los siguientes comandos muestra el estado operativo de la interfaz Gigabit 0/1 con respecto al *trunking* VLAN?

a. show interfaces gi0/1

b. show interfaces gi0/1 switchport

c. show interfaces gi0/1 trunk

d. show trunks

9. Un ingeniero acaba de instalar cuatro nuevos switches 2960 y los ha conectado entre si utilizando cables cruzados. Todas las interfaces están en un estado "up y up". El ingeniero configura cada switch con el nombre de dominio VTP Fred y deja los cuatro switches en el modo de servidor VTP. El ingeniero añade la VLAN 33 a las 9:00 de la mañana, y después de 30 segundos, ejecuta el comando show vlan brief en los otros tres switches, pero no encuentra la VLAN 33 en ellos. ¿Qué respuesta da la razón más probable que explique lo que está pasando en este caso?

a. VTP necesita que todos los switches tengan la misma contraseña VTP.

b. El ingeniero debe tener más paciencia y esperar a que el SW1 envíe su siguiente actualización periódica de VTP.

c. Ninguno de los enlaces entre switches se hace troncal, porque el modo administrativo troncal del 2960 es auto.

d. Ninguna respuesta es correcta.

10. Los switches SW1 y SW2 están conectados por un troncal operativo. El ingeniero quiere utilizar VTP para comunicar cambios de configuración de la VLAN. El ingeniero configura una nueva VLAN en SW1, VLAN 44, pero SW2 no aprende la nue-

va VLAN. ¿Cuál de los siguientes valores de configuración en SW1 y en SW2 no podrían ser la causa potencial por la cual SW2 no aprende acerca de la VLAN 44?

a. Nombres de dominio de VTP larry y LARRY, respectivamente.

b. Contraseñas VTP bob y BOB, respectivamente.

c. *Pruning* VTP habilitado y deshabilitado, respectivamente.

d. Modos VTP servidor y cliente, respectivamente.

Temas fundamentales

Un switch Catalyst de Cisco utiliza valores predeterminados que le permiten funcionar sin necesidad de realizar configuración adicional alguna. No obstante, la mayoría de las instalaciones configuran tres tipos de características del switch: las VLANs, tratadas en este capítulo; el árbol de extensión, que se trata en el Capítulo 2; y una variedad de opciones administrativas que no tienen impacto en la tarea de reenvío del switch, que se explicaron en la *Guía del Examen de Certificación Oficial CCENT/CCNA ICND1*.

Todos los objetivos publicados para el examen ICND1 se consideran prerrequisitos para el examen ICND2, aunque el examen ICND2 no trata estos temas como un fin en sí mismos. Por ejemplo, como se describe en el libro ICND1, los switches aprenden direcciones MAC examinando la dirección MAC de origen de las tramas, y tomando las decisiones de reenvío/filtrado basándose en las direcciones MAC de destino de las tramas. Esos capítulos del libro dedicados a las LANs (Capítulo 3 más los Capítulos 7 hasta el 11) también explican los conceptos de autonegociación, colisiones, dominios de colisión y dominios de difusión. Así, mientras el examen ICND2 puede no tener una pregunta específica sobre estos temas, estos temas pueden ser necesarios para contestar a una pregunta relativa a los objetivos del examen ICND2. Y, por supuesto, el examen CCNA cubre todos los temas y objetivos de ambos exámenes, ICND1 e ICND2.

Además de los conceptos básicos, el libro ICND1 también describe una amplia variedad de pequeñas tareas de configuración que o proporcionan acceso a cada switch o ayudan a proteger el switch cuando se permite el acceso. Un switch puede configurarse con una dirección IP, una máscara de subred, y un *gateway* predeterminado permitiendo acceso remoto al mismo. Junto con este acceso, Cisco recomienda una serie de acciones para mejorar la seguridad más allá de proteger el acceso físico al router para prevenir el acceso desde la consola del switch. En concreto, se pueden configurar contraseñas, y para accesos remotos utilizar si es posible Shell Segura (SSH) en lugar de Telnet. El servicio HTTP podría también ser deshabilitado, y se podrían configurar avisos de potenciales ataques. Además, los mensajes de *syslog* de cada switch se podrán monitorizar en busca de mensajes relativos a varios tipos de ataques.

Los tres capítulos de esta primera parte del libro recogen la historia de las LAN, explicando los temas relativos a los objetivos del examen ICND2. En concreto, este capítulo examina los conceptos relativos a las VLAN y cubre la configuración y operación de las VLANs. La primera sección principal de este capítulo explica los conceptos centrales,

incluyendo cómo circula el tráfico de VLAN entre switches utilizando troncales de VLAN, y cómo el Protocolo de *trunking* VLAN (VTP, *VLAN Trunking Protocol*) propietario de Cisco ayuda al proceso de configurar VLANs en un campus. La segunda sección principal de este capítulo muestra cómo configurar VLANs y troncales de VLAN, cómo asignar de forma estática interfaces a una VLAN, y cómo configurar un switch para que un teléfono o un PC en la misma interfaz estén en dos VLANs diferentes. La sección principal final cubre la configuración y resolución de problemas de VTP.

Conceptos de LANs virtuales

Antes de definir las VLANs, se debe entender la definición de LAN. Aunque se puede pensar en las LANs desde muchas perspectivas, una en particular ayuda a entender las VLANs:

Una LAN incluye todos los dispositivos del mismo dominio de difusión.

Un dominio de difusión incluye el conjunto de todos los dispositivos conectados a la LAN que cuando un dispositivo envía una trama de difusión, todos los demás dispositivos la reciben. Por tanto, se puede pensar que una LAN y un dominio de difusión son la misma cosa.

Sin VLANs, un switch considera que todas sus interfaces están en el mismo dominio de difusión; en otras palabras, todos los dispositivos conectados están en la misma LAN. Con VLANs, un switch puede poner algunas interfaces en el mismo dominio de difusión que otras, creando múltiples dominios de difusión. Estos dominios de difusión individuales creados por el switch se denominan LANs virtuales. La Figura 1.1 muestra un ejemplo, con dos VLANs y dos dispositivos en cada una.

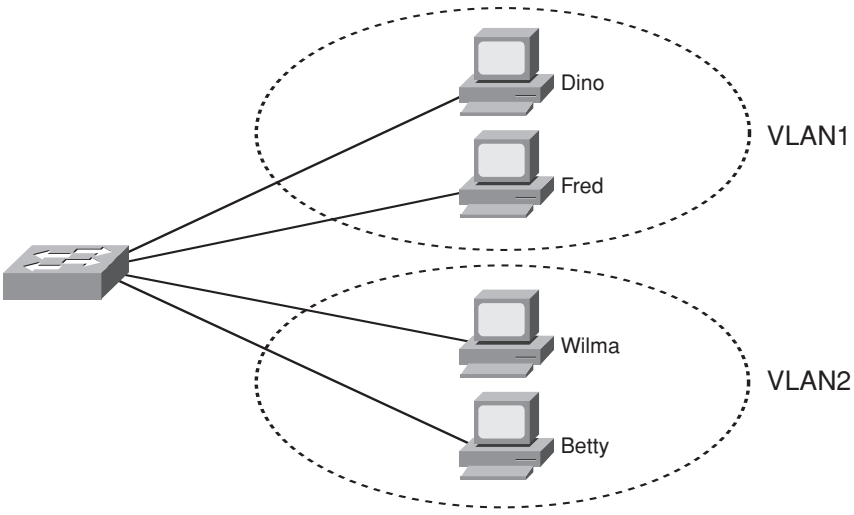


Figura 1.1. Red de ejemplo con dos VLANs utilizando un switch.

Situar hosts en dos VLANs diferentes proporciona muchos beneficios, aunque las razones pueden no ser obvias en la Figura 1.1. La clave para apreciar estos beneficios es comprender que una difusión enviada por un hosts en la VLAN será recibida y procesada por todos los demás hosts de la VLAN, pero no por los hosts de una VLAN diferente. Cuantos más hosts haya en una VLAN dada, mayor será el número de difusiones y por tanto mayor será el tiempo de procesamiento que va a requerir cada uno de los hosts de esa VLAN. Además, cualquiera puede obtener paquetes de software libre, llamados genéricamente analizadores de protocolos, con los cuales capturar todas las tramas recibidas por un host. (Visite Wireshark, en http://www.wireshark.org, para obtener un buen paquete analizador gratuito). Como resultado, las grandes VLANs producen gran número y tipos de difusiones a los otros equipos, produciendo más tramas en los hosts que podrían ser usadas por un atacante que utilice un software analizador de protocolos para tratar de realizar un ataque. Éstas son sólo unas pocas razones para separar hosts en VLANs diferentes. Las razones más comunes son las siguientes:

Tema clave

- Crear diseños más flexibles que agrupen a usuarios por departamentos, o por grupos que trabajen juntos, en lugar de por su ubicación física.
- Segmentar dispositivos en LANs más pequeñas (dominios de difusión) para reducir la sobrecarga causada por cada host en la VLAN.
- Reducir la carga de trabajo del Protocolo de árbol de extensión (STP, *Spanning Tree Protocol*) limitando una VLAN a un único acceso al switch.
- Forzar una mayor seguridad separando los hosts que trabajen con datos sensibles en una VLAN diferente.
- Separar tráfico enviado por un teléfono IP del tráfico enviado por PCs conectados a los teléfonos.

Este capítulo no examina las razones para las VLANs en mayor profundidad, pero examina estrechamente cómo trabajan las VLANs a través de varios switches de Cisco, incluyendo la configuración necesaria. Con este fin, la siguiente sección examina el *trunking* VLAN, una función necesaria cuando se instala una VLAN en más de un switch LAN.

Trunking con ISL y 802.1Q

Cuando se utilizan VLANs en una red con varios switches interconectados, los switches deben usar el *trunking* VLAN en los segmentos entre los switches. Este proceso permite a los switches utilizar el proceso denominado etiquetado de VLAN (*VLAN tagging*), por el cual el switch emisor añade otro encabezado a la trama antes de enviarla por el troncal. Este encabezado VLAN extra incluye un campo identificador de VLAN (ID VLAN) por el cual el switch emisor puede mostrar el ID de la VLAN y el switch receptor puede entonces conocer a qué VLAN pertenece cada trama. La Figura 1.2 esboza la idea básica.

El uso del *trunking* permite a los switches pasar tramas procedentes de varias VLANs a través de una única conexión física. Por ejemplo, la Figura 1.2 muestra al

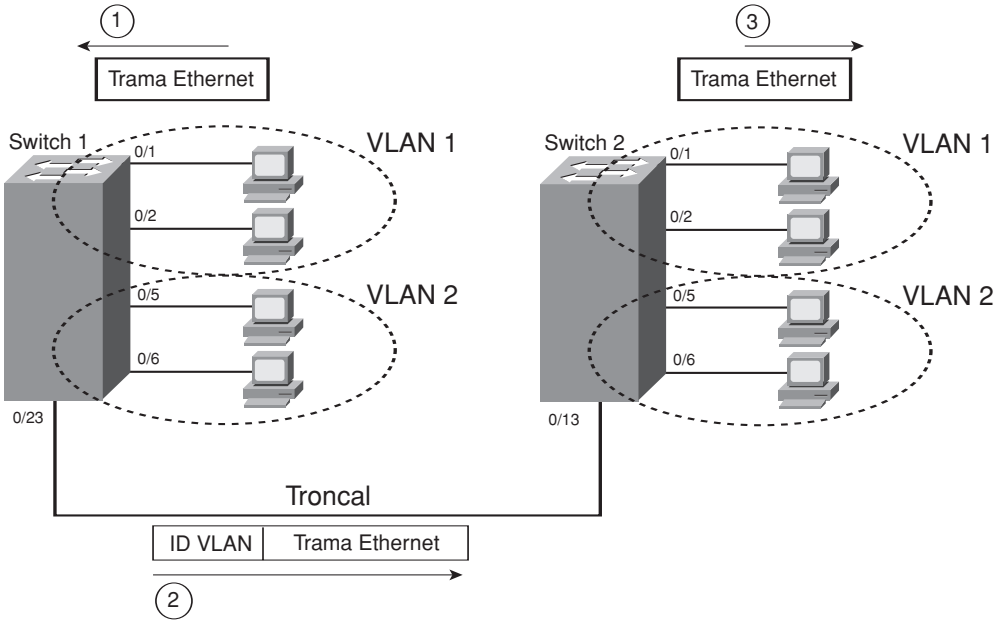


Figura 1.2. *Trunking* de VLAN entre dos switches.

switch 1 recibiendo una trama de difusión por la interfaz Fa0/1 en el Paso 1. Para inundar la trama, el switch 1 necesita enviar la trama de difusión al switch 2. Sin embargo, el switch 1 necesita que el switch 2 conozca que la trama es parte de la VLAN 1. Por tanto, como se muestra en el Paso 2, antes de enviar la trama, el switch 1 añade una cabecera VLAN a la trama Ethernet original, con una lista de identificadores de VLAN, en este caso un ID VLAN de 1. Cuando el switch 2 recibe la trama, ve que la trama es de un elemento en la VLAN 1; por tanto, el switch 2 sólo enviará la difusión por sus propias interfaces que pertenezcan a la VLAN 1. El switch 2 elimina la cabecera VLAN, enviando la trama original por sus interfaces en VLAN 1 (Paso 3).

Para otro ejemplo, considérese el caso en el que el dispositivo en la interfaz Fa0/5 del switch 1 envía una difusión. El switch 1 envía la difusión por el puerto Fa0/6 (porque este puerto está en la VLAN 2) y por Fa0/23 (porque es un troncal, es decir, soporta múltiples VLANs diferentes). El switch 1 añade la cabecera de troncal a la trama, con un ID VLAN de 2. El switch 2 elimina la cabecera de troncal después de anotar que la trama es parte de la VLAN 2; por tanto, el switch 2 sabe que debe enviar la trama sólo por los puertos Fa0/5 y Fa0/6, y no por los puertos Fa0/1 y Fa0/2.

Los switches de Cisco soportan dos protocolos diferentes de *trunking*: Enlace entre switches (ISL, *Inter-Switch Link*) e IEEE 802.1Q. Los protocolos de *trunking* proporcionan varias características, la más importante de ellas define las cabeceras con las cuales identificar el ID VLAN, como se muestra en la Figura 1.2. Ellas presentan varias diferencias como se discutirá más adelante.

ISL

Cisco creó ISL varios años antes que el IEEE creara el protocolo de *trunking* estándar de VLAN, el 802.1Q. Debido a que ISL es propiedad de Cisco, sólo puede ser utilizado entre dos switches de Cisco que soporten ISL. (Algunos switches nuevos de Cisco ya no soportan ISL; en cambio sólo soportan la alternativa estándar, 802.1Q). ISL encapsula completamente la trama Ethernet original en una cabecera y una información final ISL. La trama Ethernet original dentro de la cabecera y la información final de ISL permanece inalterada. La Figura 1.3 muestra el entramado de ISL.

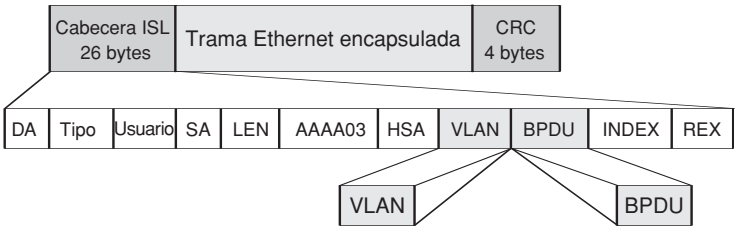


Figura 1.3. Cabecera ISL.

La cabecera ISL incluye varios campos, pero lo más importante es que el campo VLAN de la cabecera ISL proporciona un lugar para codificar el número de VLAN. Etiquetando una trama con el número correcto de VLAN en la cabecera, el switch que envía puede asegurar que el switch receptor conoce a qué VLAN pertenece la trama encapsulada. También las direcciones de origen y destino en la cabecera ISL utilizan las direcciones MAC del switch que envía y del que recibe, en oposición a los dispositivos que realmente envían la trama original. Aparte de esto, los detalles de la cabecera ISL no son importantes.

IEEE 802.1Q

El IEEE estandariza muchos de los protocolos relativos a las LAN, y el *trunking* VLAN no es una excepción. Años antes que Cisco creara ISL, el IEEE completa el trabajo en el estándar 802.1Q, que define las diferentes maneras de realizar el *trunking*. Hoy, 802.1Q ha llegado a ser el más popular de los protocolos de *trunking*. Cisco ya no soporta ISL en algunos de sus nuevos modelos de switches para LAN, incluyendo los switches 2960 utilizados en los ejemplos de este libro.

802.1Q utiliza un estilo diferente de cabecera que el utilizado por ISL para etiquetar las tramas con un número de VLAN. De hecho, 802.1Q no encapsula realmente la trama original en otra cabecera y otra información final Ethernet. En cambio, 802.1Q inserta una cabecera de VLAN extra de 4 bytes en la cabecera Ethernet de la trama original. Como resultado, al contrario de ISL, la trama tiene todavía las direcciones MAC de origen y destino originales. También, debido a que la cabecera original se ha expandido, la encapsulación de 802.1Q fuerza a recalcular el campo de secuencia de verificación de trama (FCS) en

la información final Ethernet, debido a que este campo está basado en el contenido de la trama completa. La Figura 1.4 muestra la cabecera 802.1Q y el entramado de la cabecera Ethernet revisada.

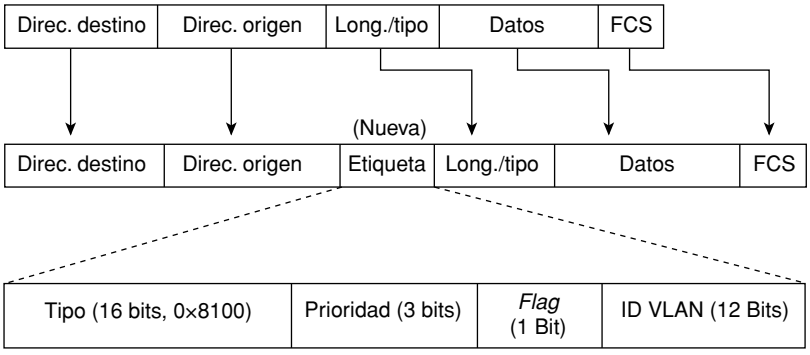


Figura 1.4. Cabecera de *trunking* 802.1Q.

Comparación de ISL con 802.1Q

Hasta ahora, el texto ha descrito la similitud entre ISL y 802.1Q, con un par de diferencias. La similitud es que ambos definen una cabecera VLAN que tiene un campo ID VLAN. No obstante, cada uno de los protocolos de *trunking* utiliza una cabecera de sobrecarga diferente, y uno está estandarizado (802.1Q) y otro es propietario (ISL). Esta sección señala algunos otros puntos importantes de comparación entre los dos.

Ambos protocolos soportan el mismo número de VLANs, concretamente 4094 VLANs. Ambos utilizan 12 bits de la cabecera VLAN para numerar las VLANs, soportando 2^{12}, ó 4096, IDs de VLAN, menos dos valores reservados (0 y 4095). De las VLANs soportadas, los IDs de VLAN de 1-1005 se consideran el *rango normal* de VLANs, mientras que los valores mayores de 1005 se denominan **rango extendido** de VLANs. Esta discusión está relacionada con el Protocolo de *trunking* VLAN (VTP, *VLAN Trunking Protocol*) que se trata en la siguiente sección.

ISL y 802.1Q soportan ambos una instancia separada del Protocolo de árbol de extensión (STP, *Spanning Tree Protocol*) para cada VLAN, pero con diferentes detalles de implementación, como se explica en el Capítulo 2. Para las LANs de campus con enlaces redundantes, el uso de una única instancia de STP significa que algunos de los enlaces permanecen inactivos en su modo normal de operación. Estos enlaces sólo se utilizan cuando otro falla. Soportando múltiples instancias de STP, los ingenieros pueden ajustar los parámetros de STP para que bajo un funcionamiento normal, parte del tráfico de las VLANs utilice un conjunto de enlaces y otro tráfico de las VLANs utilice otros enlaces, con la ventaja de usar así todos los enlaces de la red.

Nota

802.1Q no siempre ha soportado instancias múltiples de STP; por tanto, algunas referencias antiguas podrían afirmar con precisión, en este momento, que 802.1Q sólo soporta una única instancia de STP.

Una diferencia clave final entre ISL y 802.1Q que se trata aquí está relacionada con una característica denominada **VLAN nativa**. 802.1Q define una VLAN en cada troncal como la VLAN nativa, mientras que ISL no utiliza este concepto. Por defecto, la VLAN nativa de 802.1Q es la VLAN 1. Por definición, 802.1Q simplemente no añade una cabecera 802.1Q a las tramas de la VLAN nativa. Cuando un switch del otro lado del troncal recibe una trama que no tiene una cabecera 802.1Q, el switch receptor sabe que la trama pertenece a la VLAN nativa. Debido a esta conducta, ambos switches deben estar de acuerdo en qué VLAN es la nativa.

La VLAN nativa de 802.1Q proporciona algunas funciones interesantes, principalmente la conexión de dispositivos que no soportan el *trunking*. Por ejemplo, un switch de Cisco podría estar conectado a un switch que no soporte el *trunking* 802.1Q. El switch de Cisco podría enviar tramas en la VLAN nativa (significa que la trama no tiene cabecera de *trunking*); por tanto, el otro switch podría entender la trama. El concepto de VLAN nativa proporciona a los switches al menos la capacidad de reenviar tráfico de una VLAN (la VLAN nativa), lo que puede permitir algunas funciones básicas como la accesibilidad vía telnet de un switch.

La Tabla 1.2 resume las características claves y los puntos de comparación entre ISL y 802.1Q.

Tema clave

Tabla 1.2. Comparación entre ISL y 802.1Q.

Función	ISL	802.1Q
Definido por	Cisco	IEEE
Inserta otros 4 bytes en la cabecera en vez de encapsular completamente la trama original	No	Sí
Soporta rango normal (1-1005) y extendido (1006-4094) de VLANs	Sí	Sí
Permite múltiples árboles de extensión	Sí	Sí
Utiliza VLAN nativa	No	Sí

Subredes IP y VLANs

Cuando se incluyen VLANs en un diseño, los dispositivos de una VLAN necesitan estar en la misma subred. Siguiendo la misma lógica de diseño, los dispositivos en VLANs diferentes necesitan pertenecer a subredes diferentes.

Debido a estas reglas, mucha gente piensa que una VLAN es una subred y una subred una VLAN. Aunque no es completamente cierto, porque una VLAN es un concepto de la capa 2 y una subred es un concepto de la capa 3, la idea general es razonable porque los mismos dispositivos en una única VLAN son los mismos dispositivos en una única subred.

Como en todas las subredes IP, para que un host en una subred pueda entregar paquetes a otro host de otra subred, al menos un router debe estar involucrado. Por ejemplo, considere la Figura 1.5, donde puede verse un switch con tres VLANs, que se muestran dentro de las líneas punteadas, con alguna de la lógica utilizada cuando un host de la VLAN 1 envía un paquete IP a un host de la VLAN 2.

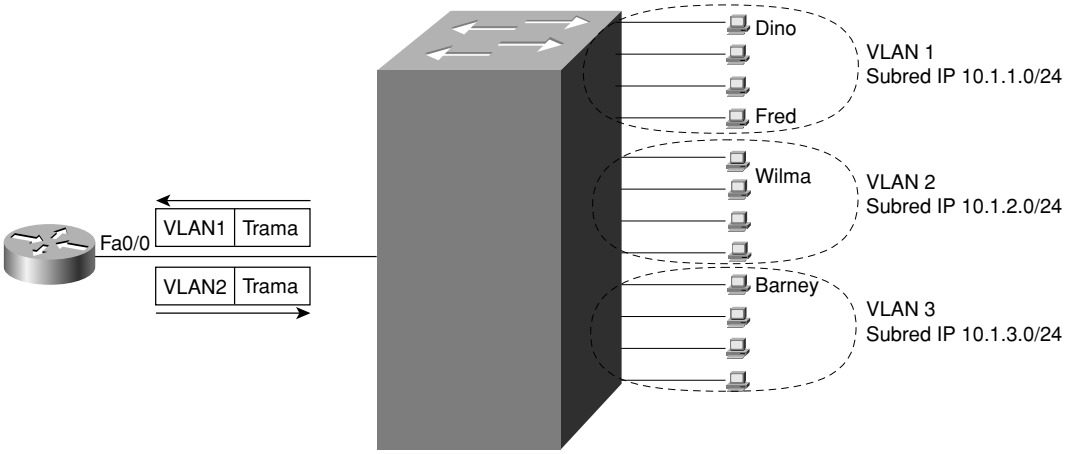


Figura 1.5. Enrutamiento entre VLANs.

En este caso, cuando Fred envía un paquete a la dirección IP de Wilma, Fred envía el paquete a su router predeterminado, ya que la dirección IP de Wilma está en una subred diferente. El router recibe la trama, con una cabecera de VLAN que implica que la trama pertenece a la VLAN 1. El router toma la decisión de enrutamiento, enviando la trama de vuelta por el mismo enlace físico, pero esta vez con una cabecera de *trunking* VLAN que indica la VLAN 2. El switch envía la trama en la VLAN 2 a Wilma.

Esto puede parecer un poco ineficiente para enviar el paquete desde el switch al router, y vuelta al switch, y así es. Una opción más adecuada en las LANs de campus es utilizar un switch, también llamado switch multicapa o switch de capa 3. Estos switches pueden realizar tanto la conmutación de capa 2 como el enrutamiento de capa 3, combinando las funciones de un router mostradas en la Figura 1.5 con las de un switch.

Protocolo de *trunking* VLAN (VTP, *VLAN Trunking Protocol*)

El Protocolo de *trunking* VLAN (VTP, *VLAN Trunking Protocol*) propietario de Cisco proporciona un mecanismo por el cual los switches de Cisco pueden intercambiar infor-

mación de la VLAN. En concreto, VTP publica sobre la existencia de cada VLAN basándose en el ID y el nombre de la VLAN. No obstante, VTP no publica los detalles sobre qué interfaces del switch están asignadas a cada VLAN.

Debido a que este libro aún no ha mostrado cómo configurar VLANs, para apreciar mejor VTP, se va a considerar este ejemplo para mostrar que es lo que VTP puede hacer. Sea una red con diez switches conectados de alguna forma utilizando troncales VLAN, y cada switch tiene al menos un puerto asignado a la VLAN con ID VLAN 3 y el nombre Contabilidad. Sin VTP, un ingeniero tiene que acceder a los diez switches y teclear los mismos dos comandos para crear la VLAN y definir sus nombres. Con VTP, se podría crear la VLAN 3 en un switch, y los otros nueve aprenderían sobre la VLAN 3 y sus nombres utilizando VTP.

VTP define un protocolo de mensajes de capa 2 que los switches utilizan para intercambiar información sobre la configuración de la VLAN. Cuando un switch cambia su configuración de VLAN (en otras palabras, cuando se añade o borra una VLAN, o cambia una ya existente) VTP sincroniza la configuración VLAN de todos los switches incluyendo los mismos IDs y nombres de VLAN. El proceso es similar a un protocolo de enrutamiento, con cada switch enviando periódicamente mensajes VTP. Los switches también envían mensajes tan pronto como su configuración de VLAN cambia. Por ejemplo, si se configura una nueva VLAN 3, con el nombre Contabilidad, el switch enviaría inmediatamente una actualización de VTP por todos los troncales, permitiendo la distribución de la información de la nueva VLAN al resto de los switches.

Cada switch utiliza uno de los tres modos de VTP: modo servidor, modo cliente, o modo transparente. Para utilizar VTP, un ingeniero configura algunos switches en modo servidor y el resto en modo cliente. Entonces, se puede añadir la configuración en los servidores, con todos los otros servidores y clientes aprendiendo acerca de los cambios en la base de datos de VLAN. Los clientes no se pueden utilizar para configurar la información de la VLAN.

De forma bastante extraña, los switches de Cisco no pueden deshabilitar VTP. La opción más parecida es utilizar el modo transparente, lo que causa que el switch ignore VTP, con la excepción de reenviar los mensajes VTP ya que otros clientes o servidores pueden recibir una copia.

La siguiente sección explica las operaciones normales cuando el ingeniero utiliza los modos servidor y cliente para obtener las ventajas de las características de VTP; a continuación se explica la forma inusual de deshabilitar esencialmente VTP habilitando el modo transparente de VTP.

Operación normal de VTP utilizando los modos servidor y cliente de VTP

El proceso de VTP comienza con la creación de la VLAN en un switch llamado servidor VTP. El servidor VTP distribuye los cambios en la configuración de la VLAN a través de mensajes VTP, enviados sólo sobre troncales ISL y 802.1Q, a lo largo de la red. Tanto los servidores como los clientes VTP procesan los mensajes VTP recibidos, actualizan sus bases

de datos de configuración de VTP basándose en estos mensajes y después envían independientemente las actualizaciones VTP por sus troncales. Al final del proceso, todos los switches aprenden la nueva información de la VLAN.

Los servidores y clientes VTP deciden si reaccionar a un mensaje de actualización VTP recibido, y actualizar sus configuraciones de VLAN basándose en si el **número de revisión de configuración de la base de datos de la VLAN** aumenta. Cada vez que un servidor VTP modifica su configuración de VLAN, el servidor VTP incrementa en 1 el número actual de revisión de la configuración. Los mensajes de actualización de VTP contienen el nuevo número de revisión de configuración. Cuando otro switch cliente o servidor recibe un mensaje VTP con un número de revisión de configuración mayor a su propio número, el switch actualiza su configuración de VLAN. La Figura 1.6 muestra cómo trabaja VTP en una red conmutada.

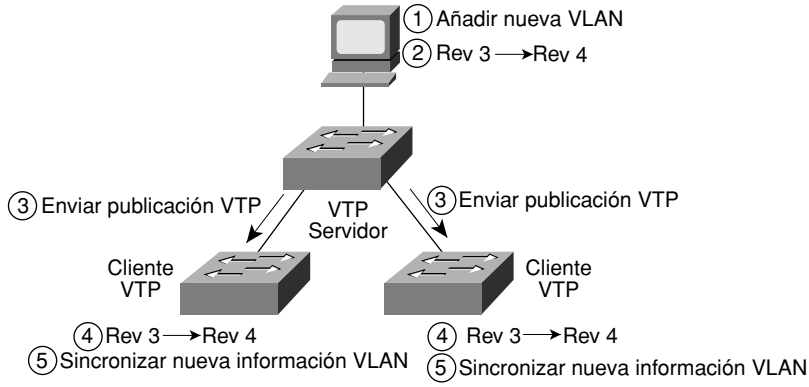


Figura 1.6. Configuración de los números de revisión de VTP y el proceso de actualización de VTP.

Inicialmente en la Figura 1.6 todos los switches tienen el mismo número de revisión de la configuración de la VLAN, lo que significa que todos tienen la misma base de datos de configuración de la VLAN; esto significa que todos los switches conocen los mismos números y nombres de VLAN. El proceso comienza cuando cada switch conoce que el número actual de revisión de la configuración es 3. Los pasos que se muestran en la Figura 1.6 son los siguientes:

1. Alguien configura la nueva VLAN desde la interfaz de línea de comandos (CLI) de un servidor VTP.
2. El servidor VTP actualiza su número de revisión de la base de datos VLAN de 3 a 4.
3. El servidor envía mensajes de actualización VTP por sus interfaces troncales, declarando el número de revisión 4.
4. Los dos switches clientes VTP comprueban que el número de revisión de la actualización (4) es mayor que su número de revisión actual (3).
5. Los dos switches clientes actualizan su base de datos VLAN basándose en las actualizaciones VTP del servidor.

Aunque este ejemplo muestra una LAN muy pequeña, el proceso trabaja igual en grandes redes. Cuando un servidor actualiza la configuración de la VLAN, el servidor envía inmediatamente mensajes VTP por todos los troncales. Los switches vecinos del otro extremo de los troncales procesan los mensajes recibidos y actualizan sus bases de datos VLAN, y después ellos envían mensajes VTP a sus vecinos. El proceso se repite en los switches vecinos, hasta que eventualmente, todos los switches han oído la nueva base de datos VLAN.

NOTA

El proceso completo por el cual un servidor cambia la configuración de la VLAN, y todos los switches VTP aprenden la nueva configuración, resultando que todos los switches conocen los mismos IDs y nombres de la VLAN, se denomina **sincronización**.

Los servidores y clientes VTP también envían periódicamente mensajes cada 5 minutos, en caso de que cualquier nuevo switch necesite conocer la configuración VLAN. Además, cuando surge un nuevo troncal, los switches pueden enviar inmediatamente un mensaje VTP solicitando a los switches vecinos el envío de sus bases de datos VLAN.

Hasta ahora, este capítulo se ha referido a los mensajes VTP como actualizaciones VTP o mensajes VTP. En la práctica, VTP define tres tipos de mensajes: publicaciones de resumen, publicaciones de subconjunto, y solicitudes de publicación. Las publicaciones de resumen listan el número de revisión, el nombre del dominio y otra información, pero no información de la VLAN. Los mensajes VTP periódicos que tienen lugar cada cinco minutos son publicaciones de resumen VTP. Si algo cambia, como lo indicado por un nuevo número de revisión mayor, el mensaje de publicación de resumen es seguido por una o más publicaciones de subconjunto, cada una de las cuales publica algún subconjunto de la base de datos VLAN. El tercer mensaje, el mensaje de solicitud de publicación, permite al switch pedir mensajes VTP a los switches vecinos tan pronto como surge el troncal. No obstante, el ejemplo mostrado para los propósitos de este libro no hace distinción en el uso de los mensajes.

Tres requisitos para que VTP funcione entre dos switches

Cuando un cliente o servidor VTP se conecta con otro cliente o servidor VTP, el IOS de Cisco necesita que se cumpla lo siguiente antes de que dos switches puedan intercambiar mensajes VTP:

- El enlace entre los switches debe trabajar como un troncal VLAN (ISL ó 802.1Q).
- El nombre de dominio VTP de los switches debe coincidir (considerando mayúsculas y minúsculas).
- Si se configura en al menos uno de los switches, las contraseñas VTP de los dos switches deben coincidir (considerando mayúsculas y minúsculas).

El nombre de dominio VTP proporciona una herramienta de diseño por la cual el ingeniero puede crear múltiples grupos de switches VTP llamados dominios, cuyas configura-

ciones de VLAN son autónomas. Para hacer esto, el ingeniero puede configurar un conjunto de switches en un dominio VTP y otro conjunto en otro dominio VTP, y los switches de los diferentes dominios ignorarán los mensajes VTP de los otros. Los dominios VTP permiten al ingeniero dividir la red conmutada en diferentes dominios administrativos. Por ejemplo, en un gran edificio con una gran plantilla de TI, una división de la plantilla de TI podría utilizar el nombre de dominio VTP de Contabilidad, mientras que otra parte podría usar el nombre de Ventas, manteniendo el control de sus configuraciones, pero haciendo posible el tráfico entre sus divisiones a través de la infraestructura de la LAN.

El mecanismo de contraseñas de VTP proporciona un medio por el cual un switch puede prevenir ataques maliciosos para obligar al switch a cambiar su configuración de VLAN. La contraseña en sí misma nunca es transmitida en texto plano o sin formato.

Cómo evitar VTP empleando el modo transparente de VTP

Es interesante saber que para evitar el uso de VTP para intercambiar información de la VLAN en los switches de Cisco, los switches no pueden deshabilitar VTP. En cambio, los switches deben utilizar el tercer modo de VTP: el modo transparente. El modo transparente otorga a un switch autonomía frente a otros switches. Como los servidores VTP, los switches en modo transparente VTP pueden configurar VLANs. No obstante, al contrario que los servidores, los switches en modo transparente nunca actualizan sus bases de datos en VLAN basándose en los mensajes VTP entrantes y los switches en modo transparente nunca tratan de crear mensajes VTP para anunciar a otros switches su propia configuración VLAN.

Los switches en modo transparente se comportan esencialmente como si VTP no existiera, sólo con una excepción: los switches en modo transparente envían las actualizaciones VTP recibidas de otros switches, simplemente para ayudar a cualquier switch servidor o cliente VTP vecino.

Desde una perspectiva de diseño, debido a los peligros asociados con VTP (se tratarán en la siguiente sección), algunos ingenieros simplemente evitan completamente VTP utilizando el modo transparente VTP en todos los switches. En otros casos, los ingenieros pueden configurar algunos switches en modo transparente para dar autonomía a los ingenieros responsables de estos switches, mientras utilizan los modos servidor y cliente en otros.

Almacenamiento de la configuración de la VLAN

Para transmitir el tráfico de una VLAN, un switch necesita conocer el ID y el nombre de las VLANs. El trabajo de VTP es publicar estos detalles, con el conjunto completo de la configuración de todas las VLANs llamado **base de datos de configuración VLAN** o simplemente base de datos VLAN.

De forma interesante, el IOS de Cisco almacena la información en la base de datos VLAN de forma diferente a la mayoría de los otros comandos de configuración del IOS de Cisco. Cuando los clientes y servidores VTP almacenan la configuración de la VLAN (con-

cretamente, el ID de la VLAN, el nombre de la VLAN, y otros valores de configuración de VTP), la configuración está almacenada en un fichero llamado vlan.dat en la memoria flash (el nombre del fichero es una abreviatura de "base de datos VLAN"). Aun más interesante es el hecho de que el IOS de Cisco no almacena esta información de configuración de la VLAN en el fichero de configuración en ejecución (*running config file*) o en el fichero de configuración de arranque (*startup-config file*). No existe ningún comando para ver directamente la configuración VTP y VLAN: en cambio, utilizando varios comandos show se puede mostrar la información sobre las VLANs y la salida VTP.

El proceso de almacenar la configuración VLAN en el fichero vlan.dat de la flash permite a ambos clientes y servidores aprender dinámicamente acerca de las VLANs, y tener la configuración automáticamente almacenada, consiguiendo por tanto que ambos estén preparados para su próxima recarga. Si las configuraciones VLAN aprendidas dinámicamente fueran añadidas solamente al fichero de configuración en ejecución (*running config file*), la LAN de campus podría estar expuesta a pérdidas de potencia en todos los switches al mismo tiempo (fácil si sólo se dispone de una fuente de alimentación en todo el edificio), perdiendo así todas las configuraciones de la VLAN. Almacenando automáticamente la configuración en el fichero vlan.dat de la memoria flash, cada switch tiene al menos una base de datos de configuración VLAN reciente y puede entonces confiar en las actualizaciones VTP de otros switches si alguna configuración VLAN ha cambiado recientemente.

Un interesante efecto colateral es que cuando se utiliza un switch cliente o servidor VTP en el laboratorio, y se desea borrar toda la configuración para arrancar un switch limpio, se debe ejecutar algo más que el comando erase startup-config. Si sólo se borra el fichero de configuración de arranque (*startup-config file*) y se reinicia el switch, el switch recuerda la configuración VLAN y VTP que está guardada en el fichero vlan.dat de la flash. Para borrar estos detalles de configuración antes de recargar el switch, se debe borrar el fichero vlan.dat de la flash con el comando delete flash:vlan.dat.

Los switches en modo transparente almacenan la configuración VLAN tanto en el fichero de configuración en ejecución (*running-config file*) como en el fichero vlan.dat de la flash. El fichero de configuración en ejecución (*running-config file*) puede guardarse en el fichero de configuración de arranque (*startup-config file*).

Nota

En algunas versiones antiguas del IOS de switch de Cisco, los servidores VTP almacenan la configuración VLAN tanto en vlan.dat como en el fichero de configuración en ejecución (*running-config file*).

Versiones de VTP

Cisco soporta tres versiones de VTP, oportunamente llamadas versiones 1, 2 y 3. La mayoría de las diferencias entre estas versiones no son importantes para su discusión en este libro. No obstante, la versión 2 de VTP cuenta con una mejora importante respecto a la versión 1 relativa al modo transparente de VTP, una mejora que se describe brevemente en esta sección.

La sección "Cómo evitar VTP empleando el modo transparente de VTP", anteriormente en este capítulo, describe cómo podría trabajar un switch con la versión 2 de VTP. Sin embargo, en la versión 1 de VTP, un switch en modo transparente podría comprobar primero el nombre de dominio y la contraseña recibidos en una actualización VTP. Si ambos parámetros no coinciden, el switch en modo transparente descarta la actualización VTP, en lugar de enviarla. El problema con la versión 1 de VTP es que en los casos donde el switch en modo transparente está instalado en una red con múltiples dominios, el switch podría no enviar todas las actualizaciones VTP. Así, la versión 2 de VTP cambia la lógica del modo transparente, ignorando el nombre de dominio y la contraseña, permitiendo a un switch con la versión 2 de VTP en modo transparente enviar todas las actualizaciones VTP recibidas.

Nota

La versión 3 está disponible sólo en los switches de gama alta y queda fuera del alcance de este libro.

Pruning VTP

Por defecto, los switches de Cisco inundan las difusiones (y las direcciones de destino desconocidas) de cada VLAN activa por todos los troncales, mientras la topología actual de STP no bloquee el troncal (Se puede encontrar más información sobre STP en el Capítulo 2.) Sin embargo, en la mayoría de las redes de campus, existen muchas VLANs en sólo unos pocos switches, pero no en todos los switches. Por tanto, es un desperdicio enviar las difusiones por todos los troncales, provocando que las tramas lleguen a los switches que no tienen ningún puerto en esa VLAN.

Los switches soportan dos métodos con los que un ingeniero puede limitar el flujo de tráfico de la VLAN en un troncal. Uno de ellos necesita la configuración manual de la **lista VLAN permitida** en cada troncal; esta configuración manual se trata más adelante en este capítulo. El segundo método, el *pruning* VTP, permite a VTP determinar dinámicamente qué switches no necesitan tramas de ciertas VLANs, y entonces VTP recorta estas VLANs en los troncales adecuados. El concepto de *pruning* simplemente significa que las interfaces apropiadas del troncal del switch no inundan tramas de esa VLAN. La Figura 1.7 muestra un ejemplo; los rectángulos de líneas discontinuas indican el troncal del cual la VLAN 10 ha sido automáticamente recortada.

En la Figura 1.7, los switches 1 y 4 tienen puertos en la VLAN 10. Con el *pruning* VTP habilitado, el switch 2 y el switch 4 utilizan VTP automáticamente para aprender que los switches de la parte inferior izquierda de la figura tienen algunos puertos asignados a la VLAN 10. Como resultado, el switch 2 y el switch 4 recortan la VLAN 10 del troncal. El recorte causa que el switch 2 y el switch 4 no envíen tramas de la VLAN 10 por esos troncales. Por ejemplo, cuando la estación A envía una difusión, los switches inundan la difusión, como muestran las flechas de la Figura 1.7.

El *pruning* VTP incrementa el ancho de banda disponible restringiendo el tráfico inundado. El *pruning* VTP es una de las dos razones principales para el uso de VTP, siendo la otra el hacer la configuración de la VLAN más fácil y consistente.

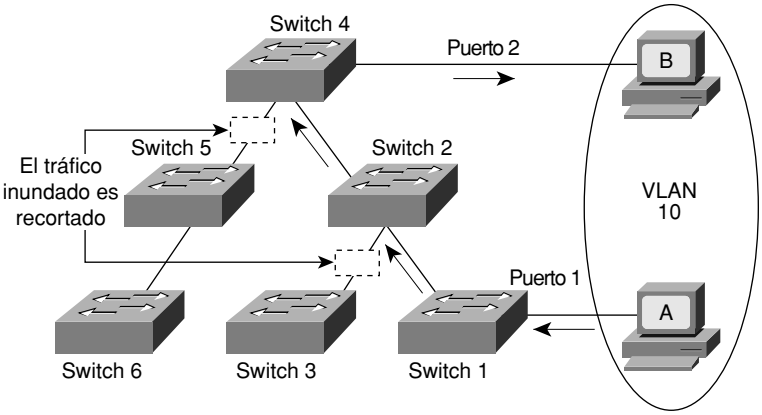


Figura 1.7. *Pruning* VTP.

Resumen de las características de VTP

La Tabla 1.3 ofrece una revisión comparativa de los tres modos de VTP.

Tabla 1.3. Características de VTP.

Función	Servidor	Cliente	Transparente
Sólo envía mensajes VTP sobre troncales ISL ó 802.1Q	Sí	Sí	Sí
Soporta la configuración CLI de las VLANs	Sí	No	Sí
Puede usar VLANs de rango normal (1-1005)	Sí	Sí	Sí
Puede usar VLANs de rango extendido (1006-4095)	No	No	Sí
Sincroniza (actualiza) sus propia base de datos de configuración cuando recibe mensajes VTP con un número de revisión mayor	Sí	Sí	No
Crea y envía actualizaciones VTP periódicas cada 5 minutos	Sí	Sí	No
No procesa las actualizaciones VTP recibidas, pero reenvía las actualizaciones VTP por otros troncales	No	No	Sí
Escribe en el fichero de la configuración en ejecución (*running-config file*) el ID de la VLAN, el nombre de la VLAN, y la configuración de VTP	No	No	Sí
Escribe en el fichero vlan.dat de la flash el ID de la VLAN, el nombre de la VLAN y la configuración de VTP	Sí	Sí	Sí

Configuración y verificación de la VLAN y del *trunking* VLAN

Los switches de Cisco no necesitan ninguna configuración para funcionar. Se pueden comprar los switches de Cisco, instalar dispositivos con el cableado correcto, encenderlos y funcionarán. Nunca necesitará configurar el switch y funcionará correctamente, a menos que se interconecten switches, o se necesite más de una VLAN. Incluso los valores predeterminados de STP podrían igualmente funcionar correctamente, pero si desea utilizar VLANs (y la mayoría de las redes empresariales lo hace) es necesario realizar alguna configuración.

Este capítulo separa los detalles de configuración de la VLAN en dos secciones principales. La sección actual se centra en las tareas de configuración y verificación cuando VTP es ignorado, bien utilizando los valores predeterminados de VTP o bien usando el modo transparente de VTP. La sección principal final de este capítulo, "Configuración y verificación de VTP", examina VTP.

Creación de VLANs y asignación de VLANs de acceso a una interfaz

Esta sección muestra cómo crear una VLAN, dando a la VLAN un nombre, y asignando interfaces a la VLAN creada. Para explicar estos detalles básicos, esta sección muestra ejemplos usando un único switch, de modo que VTP y los troncales no son necesarios.

Para que un switch de Cisco reenvíe tramas en una VLAN particular, el switch debe ser configurado para creer que la VLAN existe. Además, el switch debe tener interfaces no troncales (llamadas **interfaces de acceso**) asignadas a la VLAN y/o troncales que soporten la VLAN. Los pasos de configuración para crear la VLAN, y asignar una VLAN a una interfaz de acceso, son los siguientes. (Obsérvese que la configuración del troncal se trata más tarde en este capítulo en la sección "Configuración del *trunking* VLAN").

Paso 1 Para configurar una nueva VLAN, siga estos pasos:

Tema clave

- **a.** Desde el modo de configuración, utilice el comando de configuración global `vlan id-vlan` para crear la VLAN y poner al usuario en modo de configuración VLAN.
- **b.** (Opcional) Utilice el subcomando de VLAN `name` *nombre* para ver el nombre de la VLAN. Si no está configurado, el nombre de la VLAN es VLANZZZZ, donde ZZZZ es el ID de la VLAN, un decimal de 4 dígitos.

Paso 2 Para configurar una VLAN para cada interfaz de acceso, siga estos pasos:

- **a.** Utilice el comando `interface` para ir al modo de configuración de interfaz para cada una de las interfaces deseadas.

b. Utilice el subcomando de interfaz switchport access vlan *id-vlan* para especificar el número de VLAN asociado con esa interfaz.

c. (Opcional) Para deshabilitar el *trunking* en esa misma interfaz, asegúrese de que la interfaz es una interfaz de acceso, utilizando el subcomando de interfaz switchport mode access**.**

NOTA

Las VLANs pueden crearse y darles un nombre en el modo de configuración (como se describe en el paso 1) o utilizando una herramienta de configuración llamada modo de base de datos VLAN. El modo de base de datos VLAN no se trata en este libro, y normalmente no se trata en otros exámenes de Cisco.

NOTA

Los switches de Cisco también soportan un método dinámico de asignación de dispositivos a las VLANs, basado en las direcciones MAC del dispositivo, usando una herramienta llamada Servidor de normas de gestión de VLAN (VMPS, *VLAN Management Policy Server*). Esta herramienta rara vez se utiliza.

El proceso anterior se puede utilizar en un switch configurado en modo transparente o en un switch con todos los valores predeterminados de VTP. Como referencia, la siguiente lista esboza los valores predeterminados importantes en un switch de Cisco relativos a las VLANs y VTP. Por ahora, este capítulo asume o los valores predeterminados de VTP o VTP en modo transparente. Más tarde en este capítulo, la sección "Advertencias al cambiar la configuración predeterminada de VTP" revisa los valores predeterminados de un switch de Cisco y la implicación de cómo pasar de no utilizar VTP, basado en los valores predeterminados, a usar VTP.

- Modo servidor de VTP.
- Sin nombre de dominio VTP.
- La VLAN 1 y las VLANs 1002-1005 están configuradas automáticamente (y no pueden ser borradas).
- Todas las interfaces de acceso se asignan a la VLAN 1 (un comando implícito switchport access vlan 1).

Ejemplo 1 de configuración de VLAN: configuración completa de una VLAN

El Ejemplo 1.1 muestra el proceso de configuración para añadir una nueva VLAN y asignar interfaces de acceso a esta VLAN. La Figura 1.8 muestra la red usada en el ejemplo, con un switch LAN (SW1) y dos hosts en cada una de las tres VLANs (1, 2 y 3). El ejemplo muestra los detalles del proceso de dos pasos para la VLAN 2 y las interfaces de la VLAN 2; la configuración de la VLAN 3 se deja para el siguiente ejemplo.

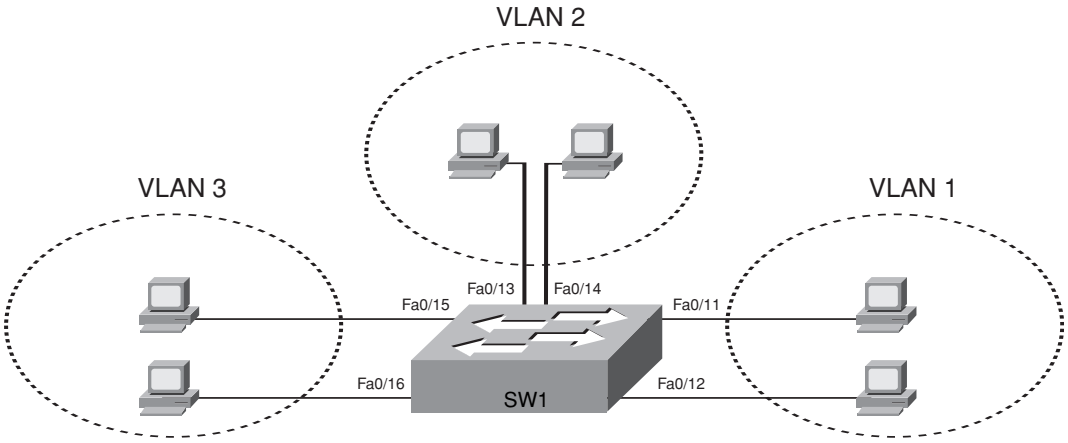


Figura 1.8. Red con un switch y tres VLANs.

Ejemplo 1.1. Configurando VLANs y asignando interfaces a las VLANs.

```
sw1-2960#show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1 default                              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
! Arriba, la VLAN 2 todavía no existe. Debajo, se añade la VLAN 2, con el nombre Freds-vlan,
! con dos interfaces asignadas a la VLAN 2.
sw1-2960#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
sw1-2960(config)#vlan 2
sw1-2960(config-vlan)#name Freds-vlan
sw1-2960(config-vlan)#exit
sw1-2960(config)#interface range fastethernet 0/13 - 14
sw1-2960(config-if)#switchport access vlan 2
sw1-2960(config-if)#exit
! Debajo, el comando show running-config muestra el subcomando de interfaz en
! las interfaces Fa0/13 y Fa0/14. Los comandos vlan 2 y name Freds-vlan
! no se muestran en la configuración en ejecución (runing-config).
sw1-2960#show running-config
! Se han omitido líneas para abreviar
interface FastEthernet0/13
switchport access vlan 2
switchport mode access
!
```

(continúa)

Ejemplo 1.1. Configurando VLANs y asignando interfaces a las VLANs *(continuación).*

```
interface FastEthernet0/14
switchport access vlan 2
switchport mode access
!
SW1#show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
2    Freds-vlan                       active    Fa0/13, Fa0/14
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

El ejemplo comienza con el comando show vlan brief, confirmando las cinco VLANs predeterminadas que no pueden borrarse, con todas sus interfaces asignadas a la VLAN 1. En concreto, se puede observar que este switch 2960 tiene 24 puertos Fast Ethernet (Fa0/1-Fa0/24) y dos puertos Gigabit Ethernet (Gi0/1 y Gi0/2), todos ellos pertenecientes a la VLAN 1.

Después, el ejemplo muestra el proceso de creación de la VLAN 2 y de asignación de las interfaces Fa0/13 y Fa0/14 a la VLAN 2. Obsérvese que este ejemplo utiliza el comando interface range, lo que provoca que el subcomando de interfaz switchport access vlan 2 se aplique a ambas interfaces en el rango, como confirma el comando show running-config al final del ejemplo.

Una vez añadida la configuración, para ver la nueva VLAN, el ejemplo repite el comando show vlan brief. Se observa como este comando muestra la VLAN 2, llamada Freds-vlan, y las interfaces asignadas a la VLAN (Fa0/13 y Fa0/14).

Nota

El Ejemplo 1.1 utiliza la configuración predeterminada de VTP. Sin embargo, si el switch ha sido configurado en el modo transparente de VTP, los comandos de configuración vlan 2 y name Freds-vlan aparecerían también en la salida del comando show running-config. Debido a que este switch VTP está en modo servidor (modo predeterminado), el switch guarda estos dos comandos sólo en el fichero vlan.dat.

En algunos casos un switch podría no utilizar la VLAN asignada por el comando switchport access vlan *id-vlan*, dependiendo del modo operativo de la interfaz. El modo operativo de un switch de Cisco está relacionado con si la interfaz está actualmente utilizando un protocolo de *trunking*. Una interfaz que está actualmente utilizando un protocolo de *trunking* se denomina **interfaz troncal**, y todas las demás se denominan **interfaces de acce-**

so. Así, los ingenieros utilizan frases como "Fa0/12 es un puerto troncal" o "Fa0/13 es una interfaz de acceso", refiriéndose a si el diseño piensa utilizar una interfaz como troncal (modo troncal) o para conectar sólo una VLAN (modo de acceso).

El subcomando opcional de interfaz switchport mode access le indica al switch que sólo permite a la interfaz ser una interfaz de acceso, lo que significa que la interfaz no utilizará el *trunking* y usará la VLAN de acceso asignada. Si se omite el subcomando opcional de interfaz switchport mode access, la interfaz podría negociar el uso del *trunking*, llegando a ser una interfaz de troncal e ignorando la VLAN de acceso configurada.

Ejemplo 2 de configuración de VLAN: la configuración más breve de una VLAN

El Ejemplo 1.1 muestra varios de los comandos opcionales de configuración, con el efecto colateral de ser un poco más largo de lo necesario. El Ejemplo 1.2 muestra una alternativa de configuración más breve, retomando la historia donde acabó el Ejemplo 1.1 y mostrándose la adicción de VLAN 3 (como puede verse en la Figura 1.8). Obsérvese que el SW1 no conoce la VLAN 3 al principio de este ejemplo.

Ejemplo 1.2. Ejemplo corto de configuración de VLAN (VLAN 3).

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface range Fastethernet 0/15 - 16
SW1(config-if-range)#switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
SW1(config-if-range)#^Z
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
2    Freds-vlan                       active    Fa0/13, Fa0/14
3    VLAN0003                         active    Fa0/15, Fa0/16
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW1#
```

El Ejemplo 1.2 muestra cómo un switch puede crear dinámicamente una VLAN (el equivalente del comando de configuración global vlan *id-vlan*) mientras el subcomando de interfaz switchport access vlan se refiere a una VLAN actualmente sin configurar. Al inicio de este ejemplo SW1 no conoce la VLAN 3. Cuando el subcomando de interfaz switchport

access vlan 3 se utiliza, el switch comprendiendo que la VLAN 3 no existe, y como se señala en el mensaje sombreado del ejemplo, crea la VLAN 3, con el nombre predeterminado (VLAN0003). No es necesario ningún otro paso para crear la VLAN. Al final del proceso, la VLAN 3 existe en el switch, y las interfaces Fa0/15 y Fa0/16 están en la VLAN 3, como se señala en la parte sombreada de la salida del comando show vlan brief.

A modo de recordatorio, obsérvese que algunos aspectos de la configuración que se muestran en los Ejemplos 1.1 y 1.2 se almacenan sólo en el fichero vlan.dat de la memoria flash, y otros están sólo en el fichero de configuración en ejecución (*running-config file*). En particular, los subcomandos de interfaz están en el fichero de configuración en ejecución; por tanto, para guardar la configuración podría ser necesario un comando copy running-config startup-config. Sin embargo, las definiciones de las nuevas VLANs 2 y 3 se han guardado automáticamente en el fichero vlan.dat de la flash. En la Tabla 1.7 se listan varios comandos de configuración, dónde se almacenan, y cómo confirmar los valores de configuración.

Configuración del *trunking* de VLAN

La configuración del *trunking* en los switches de Cisco involucra dos importantes opciones de configuración:

- El tipo de *trunking*: IEEE 802.1Q, ISL, o negociar cuál usar.
- El **modo administrativo**: troncal, no troncal o negociado.

Los switches de Cisco pueden negociar o configurar el tipo de *trunking* a utilizar (ISL o 802.1Q). Por defecto, los switches de Cisco negocian el tipo de *trunking* con el switch del otro extremo del troncal, utilizando el Protocolo de troncal dinámico (DTP, *Dynamic Trunk Protocol*). Cuando negocian, si ambos switches soportan ISL y 802.1Q, eligen ISL. Si un switch desea utilizar otro tipo, y el otro switch sólo puede utilizar un tipo de *trunking*, los dos switches acuerdan utilizar un tipo de *trunking* soportado por ambos. El tipo de *trunking* preferido por una interfaz, para los switches que soportan ambos tipos, se configura utilizando el subcomando de interfaz switchport trunk encapsulation {dot1q | isl | negotiate}. (Muchos de los switches de Cisco más recientemente desarrollados, incluidos los 2960, sólo soportan el *trunking* 802.1Q estándar del IEEE; por tanto, el valor predefinido de estos switches es switchport trunk encapsulation dot1q.)

El modo administrativo se refiere a los valores de configuración si en una interfaz se define el *trunking*. El término **administrativo** se refiere a lo que se configura, considerando que el modo **operativo** de la interfaz se refiere a lo que en ella está pasando. Los switches de Cisco utilizan un **modo administrativo** de la interfaz, como el configurado con el subcomando de interfaz switchport mode, para determinar si se utilizan el *trunking*. La Tabla 1.4 enumera las opciones del comando switchport mode.

Por ejemplo, considérense los dos switches de la Figura 1.9. Esta figura muestra una ampliación de la red de la Figura 1.8, con un troncal para un nuevo switch (SW2) y con partes de las VLANs 1 y 3 en puertos conectados al SW2. Los dos switches utilizan un enlace Gigabit Ethernet para el troncal. En este caso, el troncal no se forma dinámicamente de manera prede-

Tema clave

Tabla 1.4. Opciones del modo administrativo de *trunking* con el comando swithport mode.

Opciones del comando	Descripción
access	Previene el uso del *trunking*, haciendo que el puerto siempre actúe como un puerto de acceso (no troncal).
trunk	Utiliza siempre el *trunking*.
dynamic desirable	Inicia y responde a mensajes de negociación para elegir dinámicamente si comenzar a utilizar el *trunking*, y define la encapsulación de *trunking*.
dynamic auto	Espera pasivamente a recibir mensajes de negociación de troncal, momento en el que el switch responderá y negociará si utilizar el *trunking*, y si es así, el tipo de *trunking*.

terminada, porque ambos switches (2960) están de manera predeterminada en un modo administrativo **auto dinámico**, lo que significa que ningún switch inicia el proceso de negociación de troncal. Cambiando un switch al modo **dinámico deseable**, que inicia la negociación, los switches negocian el uso del *trunking*, en concreto 802.1Q ya que los 2960 sólo soportan 802.1Q.

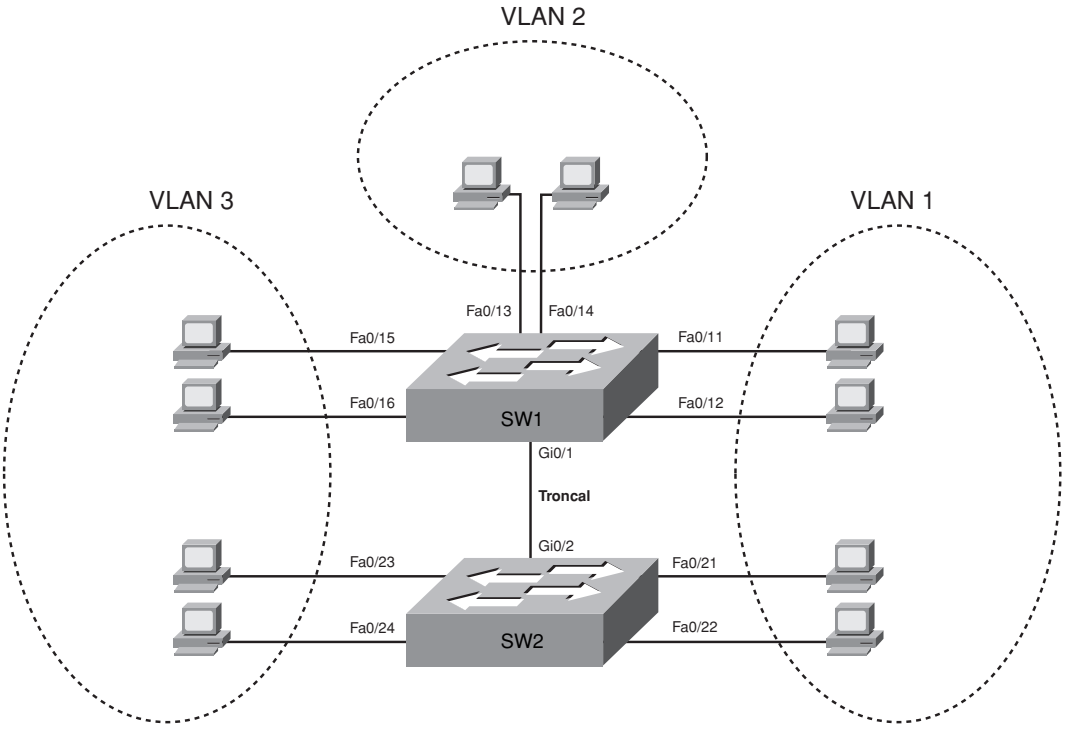


Figura 1.9. Red con dos switches y tres VLANs.

El Ejemplo 1.3 comienza mostrando los dos switches con la configuración predeterminada, por lo que los dos switches no forman el troncal. Después se muestra la configuración de SW1 para que los dos switches negocien y utilicen el *trunking* 802.1Q.

Ejemplo 1.3. Configuración de *trunking* y comandos show en los switches 2960.

```
SW1#show interfaces gigabit 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
! Obsérvese que el siguiente comando devuelve una línea en blanco.
SW1#show interfaces trunk

SW1#
! A continuación, el modo administrativo se establece como dynamic desirable.
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface gigabit 0/1
SW1(config-if)#switchport mode dynamic desirable
SW1(config-if)#^Z
SW1#
01:43:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down
SW1#
01:43:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up
```

(continúa)

Ejemplo 1.3. Configuración de *trunking* y comandos show en los switches 2960 *(continuación).*

```
SW1#show interfaces gigabit 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
! Líneas omitidas por brevedad
! El siguiente comando mostraba anteriomente una línea vacía; ahora muestra
! información de un troncal operativo.
SW1#show interfaces trunk

Port      Mode         Encapsulation     Status       Native vlan
Gi0/1     desirable    802.1q            trunking     1

Port      Vlans allowed on trunk
Gi0/1     1-4094

Port      Vlans allowed and active in management domain
Gi0/1     1-3

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/1     1-3
```

Primero, nos centraremos en los elementos importantes de la salida del comando show interfaces switchport al comienzo del Ejemplo 1.3. La salida lista el modo administrativo predeterminado establecido en auto dinámico. Ya que el SW2 también está de forma predeterminada en auto dinámico, el comando muestra el estado operativo de SW1 como acceso, lo que significa que no es troncal. La tercera línea sombreada señala el único tipo de *trunking* soportado (802.1Q) en este switch 2960. (En un switch que soporte tanto ISL como 802.1Q, este valor sería de forma predeterminada "negociado", lo que significa que el tipo o encapsulación se negociaría.) Finalmente, el tipo de *trunking* operativo se lista como "nativo", que es una manera sutil de decir que el switch no añade ninguna cabecera de *trunking* para reenviar las tramas en este puerto, tratando las tramas como si fueran de una VLAN nativa 802.1Q.

Para habilitar el *trunking*, el modo administrativo de los dos switches debe establecerse a una combinación de valores que resulten en el *trunking*. Cambiando el SW1 para que utilice el modo dinámico deseado, como se muestra en el Ejemplo 1.3, el SW1 podrá ahora iniciar la negociación, y los dos switches podrán utilizar el *trunking*. Es de particular interés el hecho de que el switch coloca la interfaz en un estado inactivo, y después la activa de nuevo, como resultado del cambio al modo administrativo de la interfaz.

Para verificar que el *trunking* está funcionando, al final del Ejemplo 1.3 se ejecuta el comando show interfaces switchport. Obsérvese que el comando todavía lista los ajustes administrativos, que denotan los valores configurados, junto con los valores operativos, que enumeran lo que el switch está haciendo actualmente. En este caso, el SW1 ahora exige estar en un modo operativo de troncal, con una encapsulación de *trunking* operativa de dot1Q.

Para los exámenes ICND2 y CCNA, deberá estar preparado para interpretar la salida del comando show interfaces switchport, comprendiendo el modo administrativo implicado por la salida, y conociendo si el enlace podría operar como troncal basándose en esos valores. La Tabla 1.5 lista las combinaciones de los modos administrativos de *trunking* y el modo operativo esperado (troncal o acceso) resultante de los valores configurados. La tabla lista a la izquierda el modo administrativo utilizado en uno de los extremos del enlace, y el modo administrativo del switch del otro extremo en la parte superior.

Tabla 1.5. Modo operativo de trunking esperado basado en los modos administrativos configurados.

Modo administrativo	Acceso	Auto dinámico	Troncal	Dinámico deseable
acceso	Acceso	Acceso	Acceso	Acceso
auto dinámico	Acceso	Acceso	Troncal	Troncal
troncal	Acceso	Troncal	Troncal	Troncal
dinámico deseable	Acceso	Troncal	Troncal	Troncal

Control de las VLANs soportadas en un troncal

La característica **lista de VLAN permitida** proporciona un mecanismo a los ingenieros para desactivar administrativamente una VLAN de un troncal. Por defecto, los switches incluyen a todas las posibles VLANs (1-4094) en la lista VLAN permitida en cada troncal. Sin embargo, el ingeniero puede limitar las VLANs permitidas en el troncal utilizando el siguiente subcomando de interfaz:

```
switchport trunk allowed vlan {add ¦ all ¦ except ¦ remove} lista-vlan
```

Este comando proporciona una manera fácil de añadir y eliminar VLANs de la lista. Por ejemplo, la opción add permite al switch añadir VLANs a la lista VLAN existente permitida, y la opción remove permite eliminar VLANs de la lista existente. La opción all significa todas las VLANs; por tanto, se puede utilizar para reiniciar el switch a sus valores predeterminados (permitiendo las VLANs 1-4094 en el troncal). La opción except es bastante difícil: añade todas las VLANs a la lista que no son parte del comando. Por ejemplo, el subcomando de interfaz switchport trunk allowed vlan except 100-200 añade las VLANs 1 a 99 y 201 a 4094 a la lista existente de VLANs permitidas en ese troncal.

Además de la lista de VLANs permitidas, un switch tiene otras tres razones para prevenir el tráfico que cruza un troncal procedente de una determinada VLAN. Las cuatro razones se resumen en la siguiente lista:

- Una VLAN ha sido eliminada de la lista de VLANs permitidas del troncal.
- Una VLAN no existe, o no está activa, en la base de datos VLAN del switch (como puede verse con el comando show vlan).
- Una VLAN ha sido recortada automáticamente por VTP.

- Una instancia de STP de la VLAN ha colocado a la interfaz del troncal en otro estado que no es el Estado de Reenvío.

Tema clave

De estas tres razones adicionales, la segunda necesita una pequeña explicación. (La tercera razón, la referida al *pruning* VTP, ya ha sido tratada en este capítulo, y la cuarta, STP, se trata completamente en el Capítulo 2.) Si un switch no conoce que una VLAN existe, como evidencia la ausencia de VLANs en la salida del comando show vlan, el switch no reenviará tramas de esa VLAN a través de ninguna interfaz. Además, una VLAN puede ser administrativamente cerrada en cualquier switch utilizando el comando de configuración global shutdown vlan *id-vlan*, el cual también provoca que el switch no reenvie nunca más tramas de esa VLAN, incluso por los troncales. Por tanto, los switches no reenvían tramas de una VLAN inexistente o cerrada sobre ninguno de los troncales del switch.

El libro enumera las cuatro razones para limitar las VLANs en un troncal en el mismo orden en el cual el IOS describe estas razones en la salida del comando show interfaces trunk. Este comando incluye una progresión de tres listas de las VLANs soportadas sobre un troncal. Estas tres listas son las siguientes:

- VLANs en la lista VLAN permitida en el troncal.
- VLANs en el grupo previo que están también configuradas y activas (no cerradas) en el switch.
- VLANs en el grupo previo que no han sido también recortadas y están en un estado STP de reenvío.

Para tener una idea de estas tres listas en la salida del comando show interfaces trunk, el Ejemplo 1.4 muestra cómo las VLANs podrían deshabilitarse en un troncal por varias razones. La salida del comando está tomada de SW1 en la Figura 1.9, después de realizar la configuración como se muestra en los Ejemplos 1.1, 1.2, y 1.3. En otras palabras, las VLANS 1 hasta la 3 existen, y el *trunking* está operativo. Entonces, durante el ejemplo, los siguientes elementos se han configurado en SW1:

Paso 1 Se añade la LAN 4.

Paso 2 La VLAN 2 se cierra.

Paso 3 La VLAN 3 se elimina de la lista VLAN permitida del troncal.

Ejemplo 1.4. Lista VLANs permitida y lista de VLANs activas.

```
! Las tres listas de VLAN del siguiente comando listan las VLANs permitidas (1-4094),
! VLANs permitidas y activas (1-3), y VLANs permitidas/activas/no recortadas/reenvío
! STP (1-3)
SW1#show interfaces trunk

Port        Mode             Encapsulation    Status      Native vlan
Gi0/1       desirable        802.1q           trunking    1
```

(continúa)

Ejemplo 1.4. Lista VLAN permitida y lista de VLANs activas *(continuación).*

```
Port        Vlans allowed on trunk
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Gi0/1       1-3

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       1-3

! A continuación, el switch se configura con la nueva VLAN 4; la VLAN 2 se cierra;
! y la VLAN 3 se elimina de la lista de VLANs permitidas en el troncal.
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#vlan 4
SW1(config-vlan)#vlan 2
SW1(config-vlan)#shutdown
SW1(config-vlan)#interface gi0/1
SW1(config-if)#switchport trunk allowed vlan remove 3
SW1(config-if)#^Z
! Las tres listas de VLANs del siguiente comando listan las VLANs permitidas (1-2, 4-4094),
! VLANs permitidas y activas (1,4), y VLANs permitidas/activas/no recortadas/reenvío
! STP (1,4)
SW1#show interfaces trunk

Port        Mode             Encapsulation    Status      Native vlan
Gi0/1       desirable        802.1q           trunking 1

! VLAN 3 se omite a continuación, porque fue eliminada de la lista de VLANs permitidas.
Port        Vlans allowed on trunk
Gi0/1       1-2,4-4094

! La VLAN 2 se omite debajo porque está cerrada. Las VLANs 5-4094 se omiten debajo
! porque SW1 no las tiene configuradas.
Port        Vlans allowed and active in management domain
Gi0/1       1,4

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       1,4
```

Trunking para los teléfonos IP de Cisco

Los teléfonos IP de Cisco utilizan Ethernet para conectar redes IP con el propósito de enviar paquetes de Voz sobre IP (VoIP). Los teléfonos IP de Cisco pueden enviar paquetes VoIP a otros teléfonos IP para soportar las llamadas de voz, así como enviar paquetes VoIP a gateways de voz, que a su vez conectan con la red telefónica tradicional existente, pudiendo hablar con cualquier otro teléfono del mundo.

Cisco anticipó que cualquier mesa de una empresa podría tener un teléfono IP de Cisco y un PC. Para reducir el desorden de los cables, Cisco incluye un pequeño switch LAN debajo de cada teléfono IP de Cisco. El pequeño switch permite que el cable procedente del cableado general más próximo a la mesa se conecte al teléfono IP y después el PC se conecta al switch con un pequeño cable Ethernet (directo) desde el PC al teléfono IP. La Figura 1.10 muestra el cableado así como algunos pequeños detalles más.

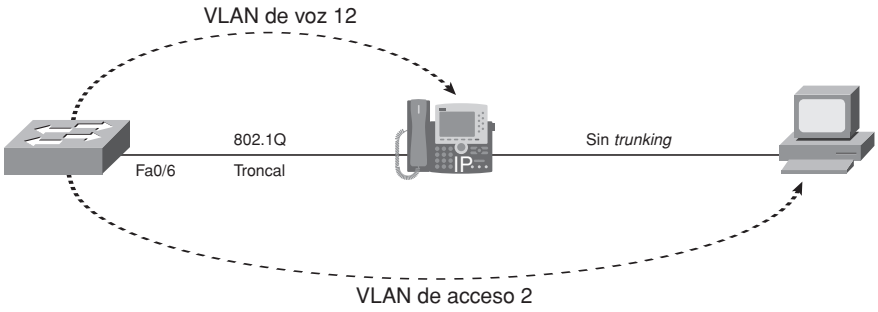


Figura 1.10. Conexión típica de un teléfono IP de Cisco y un PC a un switch de Cisco.

Las guías de diseño de telefonía IP de Cisco sugieren que el enlace entre el teléfono y el switch utilice el troncal 802.1Q, y que el teléfono y el PC estén en VLANs diferentes (y, por tanto, en diferentes subredes). Colocando los teléfonos en una VLAN, y los PCs conectados a los teléfonos en diferentes VLANs, los ingenieros pueden gestionar más fácilmente el espacio de direcciones IP, aplicar más fácilmente mecanismos de calidad de servicio (QoS, *quality of service*) a los paquetes VoIP, y proporcionar mayor seguridad separando el tráfico de datos del de voz.

Cisco denomina a la VLAN utilizada en el tráfico telefónico la VLAN de voz y a la VLAN utilizada para datos la VLAN de datos o de acceso. Para que el switch pueda reenviar el tráfico correctamente, los switches de Cisco necesitan conocer el ID VLAN de ambas, la VLAN de voz y la de datos. La VLAN de datos (o de acceso) se configura nada más consultar los últimos ejemplos, utilizando el comando switchport access vlan *id-vlan*. La VLAN de voz se configura con el subcomando de interfaz switchport voice vlan *id-vlan*. Por ejemplo, para la Figura 1.10, la interfaz Fa0/6 necesitaría el subcomando de interfaz switchport access vlan 2 y el subcomando switchport voice vlan 12.

La Tabla 1.6 resume los puntos clave acerca de la VLAN de voz.

Tabla 1.6. Configuración VLAN de voz y de datos.

Dispositivo	Nombre de la VLAN	Configurar con este comando
Teléfono	VLAN de voz o auxiliar	switchport voice vlan *id-vlan*
PC	VLAN de datos o de acceso	switchport access vlan *id-vlan*

VLANs y troncales seguros

Los switches están expuestos a varios tipos de vulnerabilidades de seguridad tanto en los puertos utilizados como en los que no. Por ejemplo, un atacante podría conectar una computadora a un punto de cableado de red que está conectado a un puerto de un switch y causar problemas en la VLAN asignada a ese puerto. Además, el atacante podría negociar el *trunking* y causar muchos otros tipos de problemas, algunos relacionados con VTP.

Cisco hace una serie de recomendaciones sobre cómo proteger los puertos no utilizados de un switch. En lugar de utilizar los valores predeterminados, Cisco recomienda configurar estas interfaces como sigue:

- Deshabilitar administrativamente la interfaz no utilizada, con el subcomando de interfaz `shutdown`.
- Prevenir la negociación del *trunking* cuando el puerto está habilitado mediante el subcomando de interfaz `switchport nonegotiate` para deshabilitar la negociación, o el subcomando de interfaz `switchport mode access` para configurar estáticamente la interfaz como interfaz de acceso.
- Asignar el puerto a una VLAN no utilizada, llamada a veces **VLAN de aparcamiento**, con el subcomando de interfaz `switchport access vlan` *id-vlan*.

Francamente, sólo con cerrar la interfaz, ya no habrá ninguna exposición de seguridad, pero las otras dos tareas previenen cualquier problema inmediato si algún otro ingeniero habilita la interfaz con el comando `no shutdown`.

Después de estas recomendaciones para los puertos no utilizados, Cisco recomienda deshabilitar la negociación del *trunking* en todas las interfaces en uso, configurando todos los troncales manualmente. La exposición es que un atacante podría desconectar la computadora de un usuario legítimo del puerto RJ-45, conectando el PC del atacante, y tratar de negociar el troncal. Configurando todas las interfaces utilizadas con el subcomando de interfaz `switchport nonnegotiate`, estas interfaces no podrán decidir dinámicamente un troncal, reduciendo la exposición a problemas relacionados con el *trunking*. Para cualquier interfaz que necesite troncal, Cisco recomienda su configuración manual.

Configuración y verificación de VTP

La configuración de VTP se realiza en unos pocos y sencillos pasos, pero VTP puede causar problemas significativos, bien por unas pobres opciones accidentales de configuración o por ataques maliciosos. Las siguientes secciones primero examinan la configuración en conjunto, seguida de algunos comentarios acerca de problemas potenciales causados por los procesos VTP y finalizan con una discusión de cómo solucionar los problemas relativos a VTP.

Uso de VTP: configuración de servidores y clientes

Antes de configurar VTP, se deben elegir algunos ajustes de VTP. En particular, asumiendo que se desea hacer uso de VTP, el ingeniero necesita decidir qué switches estarán en el mismo dominio VTP, lo que significa que estos switches aprenderán de los otros la información de configuración de la VLAN. Se debe elegir el nombre del dominio VTP, junto con una contraseña opcional pero recomendada de VTP. (Ambos valores hacen distinción entre mayúsculas y minúsculas.) El ingeniero también debe elegir qué switches serán servidores (generalmente, al menos dos para tener redundancia), y cuáles serán clientes.

Una vez finalizada la planificación, se pueden utilizar los siguientes pasos para configurar VTP:

Paso 1 Configurar el modo de VTP utilizando el comando de configuración global vtp mode {server | client}.

Paso 2 Configurar el nombre del dominio VTP (sensible al uso de mayúsculas y minúsculas) con el comando de configuración global vtp domain *nombre-dominio*.

Paso 3 (Opcional) Tanto en clientes como en servidores, configurar la misma contraseña sensible al uso de mayúsculas y minúsculas con el comando de configuración global vtp password *contraseña*.

Paso 4 (Opcional) Configurar el *pruning* VTP en los servidores VTP utilizando el comando de configuración global vtp pruning.

Paso 5 (Opcional) Habilitar la versión 2 de VTP con el comando de configuración global vtp version 2.

Paso 6 Plantear los troncales entre los switches.

El Ejemplo 1.5 muestra un ejemplo de configuración, junto con un comando show vtp status, para los dos switches de la Figura 1.11. La figura muestra los ajustes de configuración en los dos switches antes de realizar la configuración de VTP. En particular, obsérvese que ambos switches utilizan los ajustes de configuración predeterminados de VTP.

Ejemplo 1.5. Configuración básica de cliente y servidor VTP.

```
! IOS genera al menos un mensaje de información después de cada comando VTP listado
! debajo. Los comentarios añadidos por el autor comienzan con un signo de exclamación.
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#vtp mode server
Setting device to VTP SERVER mode
SW1(config)#vtp domain Freds-domain
Changing VTP domain name from NULL to Freds-domain
SW1(config)#vtp password Freds-password
Setting device VLAN database password to Freds-password
SW1(config)#vtp pruning
Pruning switched on
```

(continúa)

Ejemplo 1.5. Configuración básica de cliente y servidor VTP *(continuación).*

```
SW1(config)#^Z
! Se cambia ahora a SW2
SW2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW2(config)#vtp domain Freds-domain
Domain name already set to Freds-domain.
SW2(config)#vtp password Freds-password
Setting device VLAN database password to Freds-password
SW2(config)#^Z
! La siguiente salida muestra el número de revisión de configuración 5, con 7 VLANs
! existentes (1 hasta 3, 1002 hasta 1005), como aprendidas de SW1
SW2#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : Freds-domain
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x22 0x07 0xF2 0x3A 0xF1 0x28 0xA0 0x5D
Configuration last modified by 192.168.1.105 at 3-1-93 00:28:35
! El siguiente comando muestra las VLANs conocidas; incluye las VLANs 2 y 3,
! aprendidas de SW1
SW2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1
2    Freds-vlan                       active
3    VLAN0003                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
! Se cambia ahora a SW1
! Volviendo a SW1, la siguiente salida confirma el mismo número de revisión que SW2,
! lo que significa que los dos switches han sincronizado sus bases de datos VLAN.
SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
```

(continúa)

Ejemplo 1.5. Configuración básica de cliente y servidor VTP *(continuación).*

```
Maximum VLANs supported locally    : 255
Number of existing VLANs           : 7
VTP Operating Mode                 : Server
VTP Domain Name                    : Freds-domain
VTP Pruning Mode                   : Enabled
VTP V2 Mode                        : Disabled
VTP Traps Generation               : Disabled
MD5 digest                         : 0x10 0xA0 0x57 0x3A 0xCF 0x10 0xB7 0x96
Configuration last modified by 192.168.1.105 at 3-1-93 00:28:35
Local updater ID is 192.168.1.105 on interface Vl1 (lowest numbered VLAN
interface found)
SW1#show vtp password
VTP Password: Freds-password
```

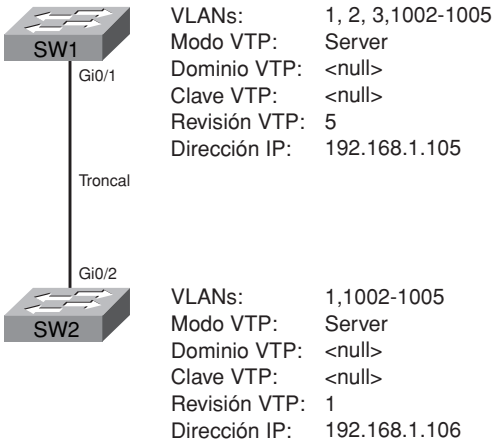


Figura 1.11. Configuración del Switch antes del Ejemplo 1.5.

El Ejemplo 1.5 muestra la siguiente configuración en SW1 y SW2, y los resultados:

- **SW1:** configurado como servidor, con el nombre de dominio VTP Freds-domain, contraseña VTP Freds-password, y *pruning* VTP habilitado.
- **SW2:** configurado como cliente, con el nombre de dominio VTP Freds-domain y la contraseña VTP Freds-password.

El ejemplo es relativamente largo, pero la configuración es directa. Ambos switches se configuraron con el modo VTP (servidor y cliente), el mismo nombre de dominio y la misma contraseña, con el *trunking* ya configurado. La configuración permite que SW2 (cliente) sincronice su base de datos VLAN para coincidir con SW1 (servidor).

El IOS de los switches de Cisco en modo servidor o cliente VTP guarda los comandos de configuración vtp, y algunos otros comandos de configuración, en el fichero vlan.dat de la flash, y los switches no guardan los comandos de configuración en el fichero de configuración en ejecución (*running-config file*). En cambio, para verificar estos comandos de con-

figuración y sus valores, se utilizan los comandos show vtp status y show vlan. A modo de referencia, la Tabla 1.7 muestra los comandos de configuración relativos a VLAN, el lugar donde servidor o cliente VTP almacenan los comandos, y cómo consultar los ajustes establecidos para los comandos.

Tema clave **Tabla 1.7.** Dónde almacenan los clientes y servidores VTP la configuración relativa a VLAN.

Comandos de configuración	Dónde se almacena	Cómo consultarlo
vtp domain	vlan.dat	show vtp status
vtp mode	vlan.dat	show vtp status
vtp password	vlan.dat	show vtp password
vtp pruning	vlan.dat	show vtp status
vla *id-vlan*	vlan.dat	show vlan [brief]
name *nombre-vlan*	vlan.dat	show vlan [brief]
switchport access vlan *id-vlan*	running-config	show running-config, show interfaces switchport
switchport voice vlan *id-vlan*	running-config	show running-config, show interfaces switchport

Cualquier análisis de VTP y de las VLANs en los switches de Cisco depende de dos comandos importantes, show vtp status y show vlan. Primero, obsérvese que cuando un dominio está sincronizado, el comando show vtp status en todos los switches debe tener el mismo número de revisión de configuración. Además, el comando show vlan debe mostrar las mismas VLANs y los mismos nombres de VLANs. Por ejemplo, SW1 y SW2 finalizan el Ejemplo 1.5 con un número de versión de 5, y ambos conocen siete VLANs: 1-3 y 1002-1005. Ambas instancias del comando show vtp status en el Ejemplo 1.5 muestran la dirección IP del último switch en modificar la base de datos VLAN (a saber, SW1, 192.168.1.105) así que es más fácil encontrar qué switch ha cambiado la configuración VLAN en último lugar. Sólo en los servidores VTP, el comando show vtp status finaliza con una línea que muestra la dirección IP del switch que lo identifica al publicar actualizaciones VTP, haciendo más fácil confirmar qué switch cambió el último la configuración de la VLAN.

Obsérvese que la contraseña sólo puede consultarse con el comando show vtp password. El comando show vtp status muestra un compendio MD5 de la contraseña.

Nota

Los switches de Cisco envían mensajes VTP y mensajes del Protocolo de descubrimiento de Cisco (CDP, *Cisco Discovery Protocol*) en los troncales utilizando la VLAN 1.

Advertencias al cambiar la configuración predeterminada de VTP

La conducta predeterminada de VTP introduce la posibilidad de problemas al configurar VTP por primera vez. Para ver por qué, considere los siguientes cinco puntos sobre VTP:

- La configuración predeterminada de VTP en los switches de Cisco es VTP en modo servidor con un nombre de dominio nulo.
- Con todos los valores predeterminados, un switch no envía actualizaciones VTP, ni siquiera por los troncales, pero el switch puede ser configurado con VLANs porque está en modo servidor.
- Después de configurar un nombre de dominio, el switch comienza inmediatamente a enviar actualizaciones VTP por todos sus troncales.
- Si un switch que todavía tiene un nombre de dominio nulo (valor predeterminado) recibe una actualización VTP (la cual por definición contiene un nombre de dominio) y no se ha utilizado contraseña en el switch que envía, el switch receptor comienza a utilizar el nombre de dominio recibido.
- Cuando tiene lugar el paso anterior, el switch con el número mayor de revisión de la base de datos VLAN hace que el switch con un número de revisión menor reescriba su base de datos VLAN.

El Ejemplo 1.5 avanza por estos cinco hechos. Comienza con el *trunking* habilitado entre dos switches, pero con configuración VTP predeterminada (los puntos 1 y 2 de la lista que precede a este párrafo). Tan pronto como SW1 configura su nombre de dominio VTP, envía mensajes VTP por el troncal a SW2 (punto 3). SW2 reacciona utilizando el nombre de dominio VTP que figura en la actualización VTP recibida (Freds-domain, en este caso). Cuando en SW2 se ejecuta el comando `vtp domain Freds-domain` en el Ejemplo 1.5, SW2 está ya utilizando el nombre de dominio aprendido dinámicamente, Freds-domain; por tanto, el IOS de Cisco de SW2 emitió la respuesta "Nombre de dominio ya establecido como Freds-domain" (punto 4). Finalmente, SW2, con un número de revisión VTP menor, sincronizó su base de datos para coincidir con la de SW1 (punto 5).

El proceso funciona exactamente como está pensado en el Ejemplo 1.5. Sin embargo, este mismo proceso permite a un ingeniero que inocentemente configure un nombre de dominio VTP dejar inoperativa la LAN conmutada. Por ejemplo, imagine que SW2 había configurado la VLAN 4 y asignado varias interfaces a la misma, pero SW1 no tiene una definición de la VLAN 4. Siguiendo este mismo proceso, cuando SW2 sincronice su base de datos VLAN para coincidir con SW1, SW2 sobrescribe la base de datos antigua, perdiendo la definición de la VLAN 4. En este punto, SW4 no podrá nunca más reenviar tramas de la VLAN 4, y todos los usuarios de la VLAN 4 comenzarán a llamar al servicio técnico.

Este mismo proceso podría utilizarse para realizar un ataque de denegación de servicio (DoS, *denial of service*) utilizando VTP. Sólo con la configuración VTP predeterminada, cualquier atacante que pueda gestionar cómo plantear un trocal entre un switch atacante y

el switch legítimo existente puede causar que los switches existentes se sincronicen con la base de datos VLAN del switch atacante, que podría muy bien no tener VLANs configuradas. Por tanto, en redes reales, si no se tiene intención de utilizar VTP cuando se instala un switch, merece la pena el esfuerzo de configurarlo para ser un switch con VTP en modo transparente, como se trata en la siguiente sección. Haciendo esto, la configuración de un nombre de dominio VTP en este nuevo switch no tendrá impacto en los switches existentes, y la configuración de un nombre de dominio en otro switch no tendrá consecuencias para este nuevo switch.

NOTA

La sección "Resolución de problemas en VTP" explica cómo reconocer cuándo VTP podría estar causando problemas como los mencionados en esta sección.

Formas de evitar VTP: configuración del modo transparente

Para evitar VTP, se necesita configurar el modo transparente de VTP. En el modo transparente, un switch nunca actualiza su base de datos VLAN basándose en los mensajes VTP recibidos, y nunca causa que otros switches actualicen sus bases de datos basándose en la base de datos VLAN de un switch en modo transparente. La única acción de VTP realizada por el switch es reenviar los mensajes VTP recibidos por un troncal por todos los otros troncales, lo que permite a otros clientes o servidores VTP funcionar correctamente.

Configurar el modo transparente de VTP es sencillo: simplemente ejecutando el comando `vtp mode transparent` en el modo de configuración global. No se necesita un nombre de dominio ni una contraseña.

Resolución de problemas de VTP

VTP puede tener un enorme impacto en una LAN de campus construida utilizando switches de Cisco, tanto negativa como positivamente. La siguiente sección examina tres aspectos de la solución de problemas en VTP. Primero, el texto sugiere un proceso con el cuál solucionar problemas de VTP cuando VTP parece no estar distribuyendo información de configuración de la VLAN (adiciones/eliminaciones/cambios). A continuación de esto, el texto examina una clase común de problemas que ocurren cuando surge un troncal, posiblemente provocando que los switches vecinos envíen actualizaciones VTP y sobrescriban la base de datos VLAN de algún switch. Este tema finaliza con sugerencias de buenas prácticas para prevenir los problemas de VTP.

Forma de averiguar por qué no funciona correctamente VTP

El primer paso en la resolución de problemas de VTP debe ser determinar en primer lugar si existe un problema. Para switches que deberían estar utilizando VTP, en el mismo dominio, se puede identificar primero un problema cuando dos switches vecinos tienen diferentes bases de datos VLAN. En otras palabras, ellos conocen IDs de VLAN diferentes, con diferentes nombres, y con un número de revisión de la configuración diferente. Después de identificar dos switches vecinos cuyas bases de datos VLAN no coinciden, el siguiente paso es verificar la configuración y el modo de *trunking* operativo (no el modo administrativo), y corregir cualquier problema. La lista siguiente detalla los pasos específicos:

Paso 1 Confirmar los nombres de switch, topología (incluyendo qué interfaces conectan qué switches), y modos VTP del switch.

Paso 2 Identificar conjuntos de dos switches vecinos que deban ser clientes o servidores VTP en los que sus bases de datos VLAN difieran mediante el comando `show vlan`.

Paso 3 En cada par de switches vecinos cuyas base de datos difieran, verificar lo siguiente:

- **a.** Al menos debe existir un troncal operativo entre los dos switches (usar el comando `show interfaces trunk`, `show interfaces switchport`, o `show cdp neighbors`).
- **b.** Los switches deben tener el mismo nombre de dominio (sensible al uso de mayúsculas y minúsculas) VTP (`show vtp status`).
- **c.** Si se configuró, los switches deben tener la misma contraseña (sensible al uso de mayúsculas y minúsculas) VTP (`show vtp password`).
- **d.** Mientras el *pruning* VTP debe estar habilitado o deshabilitado en todos los servidores del mismo dominio, tener dos servidores configurados con una configuración de *pruning* opuesta no previene el proceso de sincronización.

Paso 4 Para cada par de switches identificados en el Paso 3, solucionar el problema bien resolviendo los problemas de *truning* o reconfigurando un switch para que los nombres de dominio y las contraseñas sean los mismos.

Nota

En las LANs de campus reales, además de los puntos de esta lista, se ha de considerar también el diseño de VTP que se intenta crear.

El proceso enumera varios pasos mostrando principalmente cómo atacar el problema con los conocimientos antes tratados en este capítulo. El proceso básicamente declara que si la base de datos VLAN difiere y los switches deben ser clientes o servidores VTP es que existe

un problema (y la raíz de la causa es generalmente algún problema de configuración de VTP). Sin embargo, en el examen, puede estar obligado a deducir la respuesta basándose en la salida del comando show. Por ejemplo, considérese un problema con tres switches (SW1, SW2, y SW3) interconectados. Una pregunta de examen podría ser encontrar cualquier problema VTP en la red, basándose en la salida de los comandos show como los del Ejemplo 1.6.

NOTA

Podría ser un buen ejercicio leer el ejemplo y aplicar los pasos de resolución de problemas especificados al comienzo de esta sección antes de leer algunas de las explicaciones que siguen al ejemplo.

Ejemplo 1.6. Ejemplo de resolución de problemas de VTP.

```
SW1#show cdp neighbors
Capability Codes:  R - Router, T - Trans Bridge, B - Source Route Bridge
                   S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID            Local Intrfce    Holdtme     Capability    Platform  Port ID
SW2                  Gig 0/1          163              S I      WS-C2960-2Gig 0/2
SW3                  Gig 0/2          173              S I      WS-C3550-2Gig 0/1
SW1#show vlan brief

VLAN Name                             Status       Ports
---- -------------------------------- --------- -------------------------------
1    default                          active       Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/13, Fa0/14
                                                   Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                   Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                   Fa0/23, Fa0/24, Gi0/2
3    VLAN0003                         active       Fa0/11
4    VLAN0004                         active
5    VLAN0005                         active
49   VLAN0049                         active
50   VLAN0050                         active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
SW1#show interfaces trunk

Port        Mode           Encapsulation      Status        Native vlan
Gi0/1       desirable      802.1q             trunking      1

Port        Vlans allowed on trunk
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Gi0/1       1,3-5,49-50
```

(continúa)

Ejemplo 1.6. Ejemplo de resolución de problemas de VTP *(continuación).*

```
Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       3-5,49-50
SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 131
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Larry
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x1D 0x27 0xA9 0xF9 0x46 0xDF 0x66 0xCF
Configuration last modified by 1.1.1.3 at 3-1-93 00:33:38
! SW2 a continuación
SW2#show cdp neighbors
Capability Codes:          R - Router, T - Trans Bridge, B - Source Route Bridge
            S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID           Local Intrfce    Holdtme     Capability    Platform  Port ID
SW1                 Gig 0/2          175              S I      WS-C2960-2Gig 0/1
SW3                 Gig 0/1          155              S I      WS-C3550-2Gig 0/2
SW2#show vlan brief

VLAN Name                             Status       Ports
---- -------------------------------- --------- -------------------------------
1    default                          active       Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
3    VLAN0003 active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
SW2#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : larry
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x75 0xC5 0xDE 0xE9 0x7C 0x2D 0x8B
Configuration last modified by 1.1.1.2 at 0-0-00 00:00:00
Local updater ID is 1.1.1.2 on interface Vl1 (lowest numbered VLAN interface found)
```

(continúa)

Ejemplo 1.6. Ejemplo de resolución de problemas de VTP *(continuación).*

```
! SW3 a continuación
SW3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
3    VLAN0003                         active Fa0/13
4    VLAN0004                         active
5    VLAN0005                         active
20   VLAN20                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
SW3#show interfaces trunk

Port        Mode           Encapsulation      Status        Native vlan
Gi0/2       desirable      n-802.1q           trunking      1

Port        Vlans allowed on trunk
Gi0/2       1-4094

Port        Vlans allowed and active in management domain
Gi0/2       1,3-5,20

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/2       1,3-5,20
SW3#show vtp status
VTP Version                     : 2
Configuration Revision          : 134
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
VTP Operating Mode              : Server
VTP Domain Name                 : Larry
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x76 0x1E 0x06 0x1E 0x1C 0x46 0x59 0x75
Configuration last modified by 1.1.1.3 at 3-1-93 01:07:29
Local updater ID is 1.1.1.3 on interface Vl1 (lowest numbered VLAN interface found)
```

Para el Paso 1, los comandos show cdp neighbors y show interfaces trunk proporcionan suficiente información para confirmar la topología, así como los enlaces que están operando como troncales. El comando show interfaces trunk lista sólo las interfaces que operan como troncales. Alternativamente, el comando show interfaces switchport lista también el

modo operativo (troncal o acceso). La Figura 1.12 muestra un diagrama de la red. Obsérvese también que el enlace entre SW1 y SW3 no utiliza actualmente troncales.

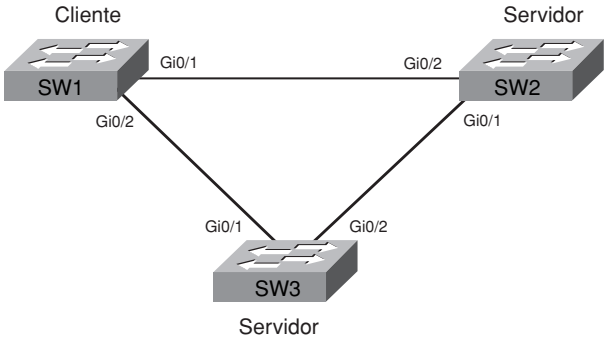


Figura 1.12. Topología de la red conmutada del Ejemplo 1.6.

Para el Paso 2, una revisión rápida de la salida del comando `show vlan brief` para cada switch muestra que los tres switches tienen diferentes bases de datos VLAN. Por ejemplo, los tres switches conocen la VLAN 3, mientras que SW1 es el único switch que conoce la VLAN 50, y SW3 es el único que conoce la VLAN 20.

Ya que los tres pares de switches vecinos tienen diferentes bases de datos VLAN, el Paso 3 del proceso de resolución de problemas sugiere examinar cada par. Comenzando con SW1 y SW2, un vistazo rápido al comando `show vtp status` en ambos identifica el problema: SW1 utiliza el nombre de dominio Larry, mientras que SW2 usa larry, y los nombres son diferentes en la primera letra (L mayúscula y l minúscula). De forma similar, SW3 y SW2 tienen dificultades por un error en su nombre de dominio VTP. Ya que SW2 es el único switch con larry en minúsculas, una solución sería reconfigurar SW2 con el nombre de dominio Larry.

Continuando el Paso 3 para SW1 y SW3, los dos switches tienen el mismo nombre de dominio (Paso 3B), pero el Paso 3A muestra que no existe un troncal que conecte SW1 con SW3. CDP confirma que la interfaz Gi0/2 de SW1 conecta con SW3, pero el comando `show interfaces trunk` en SW1 no lista la interfaz Gi0/2. Como resultado, ningún switch puede enviar mensajes VTP a los otros. La raíz de la causa de este problema está probablemente en la vigilancia de la configuración del subcomando de interfaz `switchport mode`.

Aunque el ejemplo no tiene ningún error en la contraseña VTP, es importante saber cómo validar las contraseñas. Primero, la contraseña se puede mostrar en cada switch con el comando `show vtp password`. Además, el comando `show vtp status` muestra un compendio MD5 derivado del nombre de dominio y la contraseña VTP. Por tanto, si dos switches tienen el mismo nombre de dominio y contraseña (sensibles a las mayúsculas y minúsculas), el valor del compendio MD5 que se muestra en la salida del comando `show vtp status` será el mismo. Sin embargo, si dos switches tienen compendios MD5 diferentes, se necesita examinar los nombres de dominio. Si los nombres de dominios son iguales, las contraseñas han de ser diferentes, ya que sus compendios MD5 son diferentes.

Antes de pasar al siguiente tema, hay que hacer un comentario rápido sobre la versión de VTP y cómo no debe afectar al funcionamiento de los switches. Si se examina de nuevo la salida del comando show vtp status en el Ejemplo 1.6 pueden verse las cabeceras Versión de VTP y Modo V2 Habilitado. La primera línea muestra la mayor versión de VTP soportada por el software del switch. La otra línea muestra la que el switch está utilizando actualmente. Si en un switch se configura la versión 2 de VTP mediante el comando vtp version 2, ésta sustituye a la versión 1 que es la predeterminada, pero sólo si los otros switches en el dominio soportan también esta versión. Por tanto, un error en la configuración de la versión de VTP significa que los switches funcionan, pero utilizan la versión 1 de VTP, y la línea "Modo V2 Habilitado" podría mostrar la palabra *disabled*, significando que la versión de VTP que se está utilizando es la 1.

Problemas cuando se conectan nuevos switches y surgen troncales

VTP puede funcionar bien durante meses, y de repente un día, comienzan a recibirse llamadas que describen casos en los cuales grandes grupos de usuarios no pueden utilizar la red. Después de varias comprobaciones, parece que algunas de las VLANs del campus han sido borradas. Los switches tienen todavía muchas interfaces con el comando switchport access vlan que se refieren a las VLANs ahora borradas. Ninguno de los dispositivos de esas VLANs ahora borradas funciona, porque los switches de Cisco no reenvían tramas de VLANs inexistentes.

Este escenario puede pasar de vez en cuando, principalmente cuando un switch nuevo se conecta a una red existente. Tanto si el problema pasa por accidente como por un ataque de denegación de servicio (DoS), la raíz del problema es que cuando surge un nuevo troncal VLAN (ISL o 802.1Q) entre dos switches, y los dos switches son servidores o clientes VTP, los switches se envían actualizaciones VTP entre sí. Si un switch recibe una publicación VTP que tiene el mismo nombre de dominio y fue generada con la misma contraseña VTP, uno o el otro switch sobrescriben su base de datos VLAN como parte del proceso de sincronización. Concretamente, el switch que tiene el número de versión menor sincroniza su base de datos VLAN para coincidir con el switch vecino (que tiene el número de versión mayor). Resumiendo el proceso más formalmente:

Paso 1 Confirmar que se producirá el *trunking* en el nuevo enlace (consultar la Tabla 1.5 para los detalles).

Paso 2 Confirmar que los dos switches utilizan el mismo nombre de dominio y contraseña VTP (con distinción entre mayúsculas y minúsculas).

Paso 3 Si los pasos 1 y 2 confirman que VTP funciona, el switch con el menor número de versión actualiza su base de datos VLAN para coincidir con el otro switch.

Por ejemplo, el Ejemplo 1.6 y la Figura 1.12 muestran que el enlace SW1-a-SW3 no forma el troncal. Si este enlace está configurado como troncal, SW1 y SW3 deberían enviar

mensajes VTP a los otros, usando el mismo nombre de dominio y contraseña VTP. Por tanto, un switch podría actualizar su base de datos para coincidir con la otra. El Ejemplo 1.6 muestra a SW1 con el número de revisión 131 y a SW3 con el número de revisión 134; por tanto, SW1 sobrescribirá su base de datos VLAN para coincidir con la de SW3, y por eso borra las VLANs 49 y 50. El Ejemplo 1.7 retoma la historia al final del Ejemplo 1.6, mostrando cómo surge el troncal entre SW1 y SW3, permitiendo la sincronización VTP, y provocando cambios en la base de datos VLAN de SW1.

Ejemplo 1.7. Ejemplo de resolución de problemas de VTP.

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface gi0/2
SW1(config-if)#switchport mode dynamic desirable
SW1(config-if)#^Z
SW1#
01:43:46: %SYS-5-CONFIG_I: Configured from console by console
01:43:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2,
changed state to down
SW1#01:43:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2,
changed state to up
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1
3    VLAN0003                         active Fa0/11
4    VLAN0004                         active
5    VLAN0005                         active
20   VLAN20                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

En la vida real, hay varias maneras de ayudar a reducir las oportunidades de que aparezcan estos problemas cuando se instala un nuevo switch en un dominio VTP existente. Concretamente, antes de conectar un nuevo switch a un dominio VTP existente, restablezca el número de versión del nuevo switch a 0 por alguno de los siguientes métodos:

- Configure el nuevo switch en modo transparente VTP y después vuelva al modo cliente o servidor de VTP.

- Borre el fichero vlan.dat de la flash del nuevo switch y reinicie el switch. Este fichero contiene la base de datos VLAN del switch, incluyendo el número de revisión.

Forma de evitar problemas de VTP mediante procedimientos comprobados

Además de la sugerencia de restablecer el número de versión de la base de datos VLAN antes de instalar un nuevo switch, las llamadas buenas prácticas pueden ayudar a evitar algunas de las trampas de VTP. Estas prácticas son las siguientes:

- Si no tiene intención de utilizar VTP, configure cada switch para utilizar el modo transparente.
- Si utiliza el modo servidor o cliente de VTP, utilice siempre una contraseña VTP.
- Deshabilite el *trunking* con los comandos `switchport mode access` y `switchport nonegotiate` en todas las interfaces excepto en los troncales conocidos, previniendo ataques de VTP mediante la eliminación del establecimiento dinámico de enlaces troncales.

Previniendo la negociación del *trunking* en la mayoría de los puertos, el atacante no puede nunca provocar una actualización VTP en uno de nuestros switches. Con el establecimiento de una contraseña VTP, aunque el atacante consiga que el *trunking* funcione en un switch existente, el atacante debería conocer la contraseña para hacer algún daño. Y utilizando el modo transparente, se puede evitar el tipo de problemas antes descritos, en la sección "Advertencias al cambiar la configuración predeterminada de VTP".

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 1.8 lista estos temas y el número de la página en la que se encuentra cada uno.

Tabla 1.8. Temas clave del Capítulo 1.

Tema clave	Descripción	Número de página
Lista	Razones para utilizar VLANs	10
Figura 1.2	Diagrama de *trunking* VLAN	11
Figura 1.4	Cabecera 802.IQ	13
Tabla 1.2	Comparación entre 802.IQ e ISL	14
Figura 1.6	Conceptos del proceso de sincronización de VTP	17
Lista	Requisitos para que VTP funcione entre dos switches	18
Tabla 1.3	Resumen de las características de VTP	22
Lista	Lista de verificación de la configuración para configurar VLANs y asignar interfaces	23-24
Lista	Configuración predeterminada de VTP y VLAN	24
Tabla 1.4	Opciones del comando switchport mode	29
Tabla 1.5	*Trunking* esperado resultante basándose en la configuración del comando switchport mode	32
Lista	Cuatro razones por las que un troncal no permite tráfico de una VLAN	32-33
Tabla 1.6	Configuración y terminología de VLAN de voz y de datos	35
Lista	Recomendaciones de cómo proteger los puertos no utilizados de un switch	36

(continúa)

Tabla 1.8. Temas clave del Capítulo 1 *(continuación).*

Tema clave	Descripción	Número de página
Lista	Lista de verificación de la configuración de VTP	37
Tabla 1.7	Comandos de configuración de VTP y VLAN, y dónde se almacenan	40
Lista	Proceso de resolución de problemas de VTP utilizados cuando VTP no funciona como se desea	43
Lista	Prediciendo qué pasará con VTP cuando un nuevo switch se conecte a la red	48
Lista	Buenas prácticas de VTP para prevenir los problemas de VTP	50

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD), o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas ya completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe sus respuestas con ayuda del glosario:

802.1Q, base de datos de configuración VLAN, ISL, modo administrativo de *trunking*, modo cliente VTP, modo operativo de *trunking*, modo servidor VTP, modo transparente VTP, *pruning* VTP, troncal, VLAN, vlan.dat, VTP.

Referencias de comandos

Aunque no necesariamente debe memorizar la información de las tablas de esta sección, ésta incluye una referencia de los comandos de configuración y EXEC utilizados en este capítulo. En la práctica, debería memorizar los comandos como un efecto colateral de leer el capítulo y hacer todas las actividades de esta sección de preparación del examen.

Para verificar si ha memorizado los comandos como un efecto colateral de sus otros estudios, cubra el lado izquierdo de la tabla con un trozo de papel, lea las descripciones del lado derecho y compruebe si recuerda el comando.

Tabla 1.9. Referencia de comandos de configuración del Capítulo 1.

Comando	Descripción
vlan *id-vlan*	Comando de configuración global que crea la VLAN y coloca la CLI en modo de configuración de VLAN.
name *nombre-vlan*	Subcomando de VLAN que da nombre a la VLAN.
shutdown	Subcomando de VLAN que previene que un switch pueda reenviar tráfico en esa VLAN.
shutdown vlan *id-vlan*	Comando de configuración global que administrativamente deshabilita una VLAN, previniendo al switch de reenviar tramas de esa VLAN.
vtp domain *nombre-dominio*	Comando de configuración global que define el nombre del dominio VTP.
vtp password *clave*	Comando de configuración global que define la contraseña de VTP.
vtp {server | client | transparent}	Comando de configuración global que define el modo de VTP.
vtp pruning	Comando global de configuración que le dice al servidor VTP que comunique a todos los switches que se va a utilizar el *pruning* VTP.
switchport mode {access | dynamic {auto | desirable} | trunk}	Subcomando de interfaz que configura el modo administrativo de *trunking* en la interfaz.
switchport trunk allowed vlan {add | all | except | remove} *lista-vlan*	Subcomando de interfaz que define la lista de VLANs permitidas.
switchport access vlan *id-vlan*	Subcomando de interfaz que configura estáticamente la interfaz en esa VLAN.
switchport trunk encapsulation {dot1q | isl | negotiate}	Subcomando de interfaz que define el tipo de *trunking* a utilizar asumiendo que el *trunking* está configurado o que se ha negociado.
switchport voice vlan *id-vlan*	Subcomando de interfaz que define la VLAN utilizada por las tramas enviadas a y desde un teléfono IP de Cisco.
switchport nonnegotiate	Subcomando de interfaz que deshabilita la negociación del *trunking* VLAN.

Tabla 1.10. Referencia de comandos EXEC del Capítulo 1.

Comando	Descripción
show interfaces *id-interfaz* switchport	Muestra información acerca de alguna interfaz con respecto a los valores administrativos y el estado operativo.
show interfaces *id-interfaz* trunk	Muestra información acerca de todos los troncales operativos (pero no otras interfaces), incluyendo la lista de VLANs que pueden ser reenviadas por el troncal.
show vlan [brief | id *id-vlan* | name *nombre-vlan* | summary]	Muestra información de la VLAN.
show vlan [*vlan*]	Muestra información de la VLAN.
show vtp status	Muestra la configuración y el estado de VTP.
show vtp password	Muestra la contraseña de VTP.

Este capítulo trata los siguientes temas:

Protocolo de árbol de extensión (IEEE 802.1d): Esta sección explica los conceptos centrales que hay detrás del funcionamiento de los protocolos originales STP (Protocolo de árbol de extensión) del IEEE.

STP Rápido (IEEE 802.1w): Esta sección se centra en las diferencias entre el anterior estándar de STP 802.1d y el nuevo RSTP 802.1w.

Configuración y verificación de STP: Esta sección explica cómo configurar STP en los switches Cisco IOS, y cómo verificar el estado actual de STP en cada switch e interfaz.

Resolución de problemas de STP: Esta sección sugiere un planteamiento sobre cómo predecir el rol de puerto de cada interfaz STP, prediciendo así la topología del árbol de extensión.

CAPÍTULO 2

Protocolo de árbol de extensión

Cuando en los diseños de LAN se necesitan múltiples switches, la mayoría de los ingenieros de redes incluyen segmentos Ethernet redundantes entre ellos. El objetivo es sencillo. Los switches podrían fallar, y los cables podrían cortarse o desenchufarse; si se instalan switches y cables redundantes, el servicio de red podría permanecer disponible para la mayoría de los usuarios.

Las LANs con enlaces redundantes introducen la posibilidad de que las tramas puedan formar por siempre bucles en la red. Estas tramas podrían causar problemas en el rendimiento de la red. Por tanto, las LANs utilizan el Protocolo de árbol de extensión (STP, *Spanning Tree Protocol*), el cual permite el uso de enlaces LAN redundantes mientras previene que las tramas formen bucles indefinidamente alrededor de la LAN a través de estos enlaces redundantes. Este capítulo trata STP, junto con algunos comandos de configuración utilizados para optimizar su comportamiento.

Este capítulo cubre los detalles de STP, más una nueva variante llamada Protocolo de árbol de extensión rápido (RSTP, *Rapid Spanning Tree Protocol*). El final del capítulo cubre la configuración de STP en los switches de la serie 2960, junto con algunas sugerencias sobre cómo plantear los problemas de STP en los exámenes.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las diez preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 2.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

Tabla 2.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
Protocolo de árbol de extensión (IEEE 802.1d)	1-5
STP Rápido (IEEE 802.1w)	6-7
Configuración y verificación de STP	8-9
Resolución de problemas de STP	10

1. ¿Cuáles de los siguientes estados de puerto de IEEE 802.1d son estados estables utilizados cuando STP ha completado la convergencia?
   a. Bloqueo (*Blocking*).
   b. Envío (*Forwarding*).
   c. Escucha (*Listening*).
   d. Aprendizaje (*Learning*).
   e. Descarte (*Discarding*).
2. ¿Cuáles de los siguientes estados transitorios de puerto de IEEE 802.1d se utilizan sólo durante el proceso de convergencia de STP?
   a. Bloqueo (*Blocking*).
   b. Envío (*Forwarding*).
   c. Escucha (*Listening*).
   d. Aprendizaje (*Learning*).
   e. Descarte (*Discarding*).
3. ¿Cuáles de estos IDs de puente podría ganar la elección como raíz, asumiendo que los switches con estos IDs de puente están en la misma red?
   a. 32768:0200.1111.1111
   b. 32768:0200.2222.2222
   c. 200:0200.1111.1111
   d. 200:0200.2222.2222
   e. 40,000:0200.1111.1111
4. ¿Cuál de los siguientes hechos determina cada cuanto tiempo un puente o switch no raíz envía un mensaje BPDU Hello STP 802.1d?
   a. El temporizador Hello configurado en ese switch.
   b. El temporizador Hello configurado en el switch raíz.
   c. Siempre es cada 2 segundos.
   d. El switch reacciona a las BPDUs recibidas desde el switch raíz enviando otra BPDU 2 segundos después de recibir la BPDU raíz.

5. ¿Qué característica de STP causa que una interfaz sea colocada en Estado de Reenvío (*Forwarding State*) tan pronto como la interfaz esté físicamente activa?
   a. STP.
   b. RSTP.
   c. Root Guard (protección raíz).
   d. 802.1w.
   e. PortFast.
   f. EtherChannel.
6. ¿Qué respuesta muestra el nombre del estándar del IEEE que mejora el estándar original de STP y baja el tiempo de convergencia?
   a. STP.
   b. RSTP.
   c. Root Guard (protección raíz).
   d. 802.1w.
   e. PortFast.
   f. *Trunking*.
7. ¿Cuáles de los siguientes estados de puerto de RSTP tienen el mismo nombre que un estado de puerto similar en el tradicional STP?
   a. Bloqueo (*Blocking*).
   b. Envío (*Forwarding*).
   c. Escucha (*Listening*).
   d. Aprendizaje (*Learning*).
   e. Descarte (*Discarding*).
   f. Deshabilitado (*Disabled*).
8. En un switch 2960, ¿cuáles de los siguientes comandos cambia el valor del ID del puente?
   a. spanning-tree bridge-id *valor*
   b. spanning-tree vlan *número-vlan* root {primary | secondary}
   c. spanning-tree vlan *número-vlan* priority *valor*
   d. set spanning-tree priority *valor*
9. Examine el siguiente extracto del comando show spanning-tree en un switch de Cisco:

```
Bridge ID     Priority      32771  (priority 32768 sys-id-ext 3)
              Address       0019.e86a.6f80
```

   ¿Cuál de las respuestas es verdadera con respecto al switch en el que se ejecutó el comando?
   a. La información es acerca de la instancia STP para la VLAN 1.
   b. La información es acerca de la instancia STP para la VLAN 3.

c. La salida del comando confirma que este switch no puede ser el switch raíz.

d. La salida del comando confirma que este switch es actualmente el switch raíz.

10. El switch SW3 ha recibido sólo dos BPDUs Hello, ambas del mismo switch raíz, recibidas en las dos interfaces listadas a continuación:

```
SW3#show interfaces status
Port      Name      Status       Vlan    Duplex     Speed     Type
Fa0/13              connected    3       a-half     a-100     10/100BaseTX
Gi0/1               connected    1       a-full     a-1000    1000BaseTX
```

En SW3 no se han ejecutado comandos de configuración relativos a STP. El Hello recibido por Fa0/13 muestra un coste de 10, y el Hello recibido por Gi0/1 muestra un coste de 20. ¿Cuál de estas opciones es cierta acerca de STP en SW3?

a. SW3 elegirá Fa0/13 como su puerto raíz.

b. SW3 elegirá Gi0/1 como su puerto raíz.

c. Fa0/13 de SW3 llegará a ser un puerto designado.

d. Gi0/1 de SW3 llegará a ser un puerto designado.

Temas fundamentales

Sin el Protocolo de árbol de extensión (STP), una LAN con enlaces redundantes podría causar que las tramas Ethernet formen bucles durante un periodo indefinido de tiempo. Con STP habilitado, algunos switches bloquean puertos para que esos puertos no reenvíen las tramas. STP selecciona qué puertos bloquear de forma que sólo exista un camino activo entre cualquier par de segmentos de LAN (dominios de colisión). Como resultado, las tramas alcanzan cada dispositivo sin causar los problemas creados cuando las tramas forman bucles en la red.

Este capítulo comienza explicando la necesidad del estándar STP original del IEEE y cómo funciona el estándar. La segunda sección principal explica en comparación cómo funciona el nuevo y más rápido STP Rápido (RSTP). Las otras dos secciones principales examinan respectivamente la configuración y la resolución de problemas de STP.

Protocolo de árbol de extensión (IEEE 802.1d)

IEEE 802.1d, el primer estándar público de STP, define una solución razonable al problema de las tramas que forman bucles infinitos en enlaces redundantes. Las secciones siguientes comienzan con una descripción más detallada del problema, seguida de una descripción del resultado final de cómo 802.1d STP lo resuelve. Las secciones finalizan con

una larga descripción de cómo funciona STP como un proceso distribuido en todos los switches LAN para prevenir los bucles.

Necesidad del árbol de extensión

El problema más común que puede ser evitado con el uso de STP es el de las tormentas de difusión. Las tormentas de difusión causan que las difusiones (o multidifusiones o unidifusiones con dirección de destino desconocida) formen bucles indefinidamente en una LAN. Como resultado, algunos enlaces pueden llegar a saturarse con copias inútiles de la misma trama, dejando fuera tramas buenas, así como provocar un impacto significativo en el rendimiento de los PCs de usuario final al provocar que procesen demasiadas tramas de difusión. Para ver cómo ocurre esto, la Figura 2.1 muestra una red de ejemplo en la cual Bob envía una trama de difusión. Las líneas punteadas muestran cómo los switches reenvían la trama cuando STP no existe.

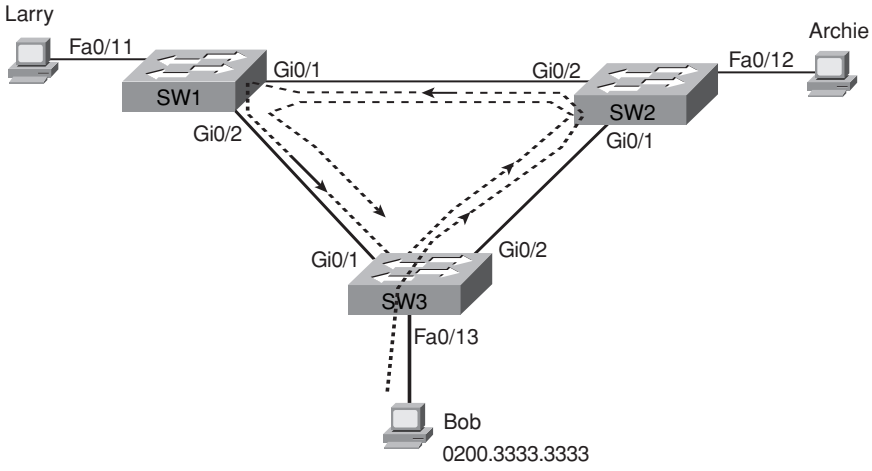


Figura 2.1. Tormenta de difusión.

Los switches inundan las difusiones por todas las interfaces de la misma VLAN, excepto por la que llegó la trama. En la figura, esto significa que SW3 reenviará la trama de Bob a SW2; SW2 enviará la trama a SW1; SW1 enviará la trama de vuelta a SW3; y SW3 enviará de nuevo la trama de vuelta a SW2. Esta trama formará bucles hasta que algo cambie (alguien cierre una interfaz, reinicie un switch, o alguna otra cosa que rompa el bucle). Obsérvese también que pasa lo mismo en la dirección opuesta. Cuando Bob envía la trama original, SW3 también reenvía una copia a SW1, SW1 reenvía a SW2, y así sucesivamente.

Como resultado de estos bucles también se produce inestabilidad en las tablas MAC. La inestabilidad en la tabla MAC significa que las tablas de direcciones MAC de los switches seguirán cambiando la información especificada para la dirección MAC de origen de

las tramas en bucle. Por ejemplo, SW3 de la Figura 2.1 comienza con una entrada en la tabla MAC como sigue:

0200.3333.3333 Fa0/13 VLAN 1

Sin embargo, piense ahora en el proceso de aprendizaje del switch que tiene lugar cuando la trama del bucle va hacia SW2, después a SW1, y después vuelve a SW3 por su interfaz Gi0/1. SW3 piensa, "¡Vaya!… la dirección MAC de origen es 0200.3333.3333, y ha llegado por la interfaz Gi0/1. ¡Actualizaré mi tabla MAC!" resultando la siguiente entrada en SW3:

0200.3333.3333 Gi0/1 VLAN 1

En este punto, si una trama llega a SW3 (una diferente a la trama en bucle que causa los problemas) destinada a la dirección MAC de Bob 0200.3333.3333, SW3 podría reenviar incorrectamente la trama por Gi0/1 a SW1. Esta nueva trama puede entrar también en bucle o simplemente no ser entregada nunca a Bob.

La tercera clase de problemas causados por no utilizar STP en una red con redundancia es que los hosts que funcionan toman múltiples copias de la misma trama. Considérese el caso en el cual Bob envía una trama a Larry, pero ninguno de los switches conoce la dirección MAC de Larry. (Los switches inundan las tramas dirigidas a una dirección MAC desconocida.) Cuando Bob envía la trama (destinada a la dirección MAC de Larry), SW3 envía una copia a SW1 y a SW2. SW1 y SW2 también inundan la trama, lo que causa que la trama entre en bucle. SW1 también envía una copia de cada trama a Larry por Fa0/11. Como resultado, Larry procesa múltiples copias de la trama, lo cual puede provocar un fallo de aplicación, e incluso algunos otros problemas de red más importantes.

La Tabla 2.2 resume las tres clases de problemas principales que ocurren cuando no se utiliza STP en una LAN con redundancia.

Tabla 2.2. Tres clases de problemas causados por no utilizar STP en LANS redundantes.

Problema	Descripción
Tormentas de difusión	El reenvío repetido de una trama en los mismos enlaces consume una parte significativa de las capacidades de los enlaces.
Inestabilidad en la tabla MAC	La actualización continua de la tabla de direcciones MAC de un switch con entradas incorrectas, como reacción a las tramas que entran en bucle, provoca que las tramas sean enviadas a localizaciones incorrectas.
Transmisión múltiple de la trama	Un efecto colateral de las tramas que entran en bucle en el cual múltiples copias de la misma trama se entregan al host previsto, confundiéndolo.

Qué hace el árbol de extensión IEEE 802.1d

STP previene bucles colocando cada puerto de un puente/switch en estado de Envío o en estado de Bloqueo. Las interfaces en estado de Envío actúan normalmente, reenviando

y recibiendo tramas, pero las interfaces en estado de Bloqueo no procesan tramas excepto los mensajes STP. Se considera que todos los puertos en estado de Envío están en el **árbol de extensión** actual. El conjunto colectivo de puertos de reenvío crea un camino único por el cual se envían las tramas entre segmentos Ethernet.

La Figura 2.2 muestra un árbol STP sencillo que resuelve el problema mostrado en la Figura 2.1 colocando un puerto de SW3 en estado de Bloqueo.

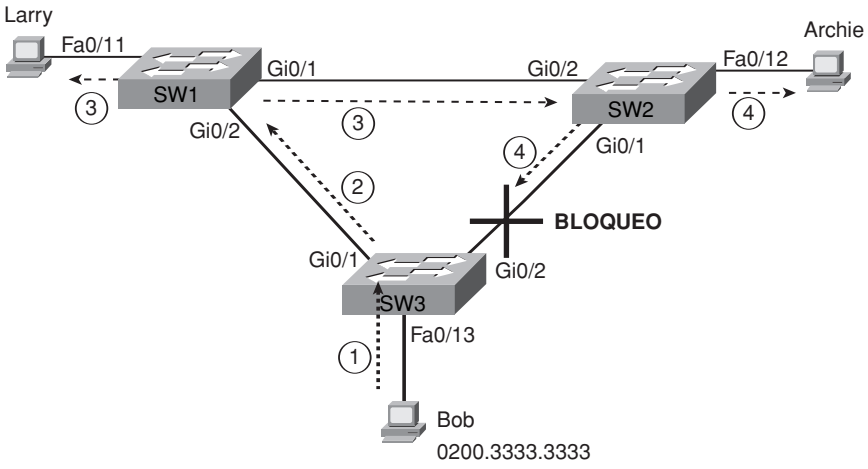


Figura 2.2. Red con enlaces redundantes y STP.

Ahora, cuando Bob envía una trama de difusión, la trama no entra en bucle. Bob envía la trama a SW3 (Paso 1), el cual reenvía entonces la trama sólo a SW1 (Paso 2), porque la interfaz Gi0/2 de SW3 está en estado de Bloqueo. SW1 inunda la trama por Fa0/11 y Gi0/1 (Paso 3). SW2 inunda la trama por Fa0/12 y Gi0/1 (Paso 4). Sin embargo, SW3 ignora la trama recibida de SW2, de nuevo porque esa trama entra por la interfaz Gi0/2 de SW3, que está en estado de Bloqueo.

Con la topología de STP de la Figura 2.2, los switches simplemente no utilizan el enlace entre SW2 y SW3 para el tráfico en esa VLAN, que es el menor de los efectos secundarios negativos de STP. Sin embargo, si el enlace entre SW1 y SW3 falla, STP converge para que SW3 envíe en lugar de bloquear su interfaz Gi0/2.

Nota

El término **convergencia de STP** se refiere al proceso por el cual los switches comprenden colectivamente que algo ha cambiado en la topología de la LAN, de modo que los switches podrían necesitar cambiar qué puertos están bloqueados y qué puertos reenvían.

¿Cómo gestiona STP el hecho de que los switches bloqueen o envíen por cada interfaz?, y ¿cómo converge para cambiar de Bloqueo a envío para aprovechar las ventajas de los

enlaces redundantes en respuesta a paradas de la red? Las siguientes secciones responden estas preguntas.

Cómo funciona el árbol de extensión

El algoritmo STP crea un árbol de extensión de interfaces que reenvían tramas. La estructura de árbol crea un camino único a y desde cada segmento Ethernet, simplemente como se puede trazar un camino único hacia una hoja, creciendo el árbol desde su base a cada hoja.

Nota

Debido a que los puentes Ethernet prácticamente no se utilizan en la actualidad, este capítulo se referirá sólo a los switches. Sin embargo, tanto los puentes como los switches utilizan STP.

El proceso utilizado por STP, a veces denominado **Algoritmo de árbol de extensión** *(STA, Spanning Tree Algorithm)*, selecciona las interfaces que serán colocadas en un estado de Envío. Para cualquier interfaz no seleccionada para estar en este estado, STA coloca las interfaces en estado de Bloqueo. Con otras palabras, STP simplemente elige qué interfaces reenviarán.

STP utiliza tres criterios para seleccionar si colocar una interfaz en estado de Envío:

- STP elige un swich raíz. STP coloca todas las interfaces operativas del switch raíz en estado de Envío.
- Cada uno de los switches no raíz considera uno de sus puertos para tener el menor coste administrativo entre sí mismo y el switch raíz. STP coloca esta interfaz de mínimo coste al raíz, llamada **puerto raíz** (*RP, Root Port*) del switch, en estado de Envío.
- Muchos switches pueden estar conectados al mismo segmento Ethernet. El switch con el coste administrativo más bajo desde sí mismo hasta el puente raíz, comparado con los otros switches conectados al mismo segmento, se coloca en estado de Envío. El switch de menor coste en cada segmento es llamado **puente designado**, y la interfaz del puente conectada a ese segmento se denomina **puerto designado** *(DP, designated port)*.

Nota

La razón real de que la raíz coloque todas sus interfaces operativas en estado de Reenvío es que todas sus interfaces llegarán a ser DPs, pero es más fácil recordar solamente que todas las interfaces operativas de los switches raíz reenviarán tramas.

Todas las demás interfaces se configuran en estado de Bloqueo. La Tabla 2.3 resume las razones de STP para configurar un puerto en estado de Envío o de Bloqueo.

Tabla 2.3. STP: razones para reenviar o bloquear.

Caracterización del puerto	Estado STP	Descripción
Todos los puertos del switch raíz	Envío	El switch raíz es siempre el switch designado en todos los segmentos a los que está conectado.
Cada puerto raíz de un switch que no es raíz	Envío	El puerto a través del cual el switch tiene el menor coste para alcanzar el switch raíz.
Cada puerto designado de la LAN	Envío	El switch que reenvía la BPDU de menor coste por el segmento es el switch designado para ese segmento.
Todos los demás puertos operativos	Bloqueo	El puerto no se utiliza para enviar tramas, ni se considerará ninguna trama recibida por estas interfaces para su envío.

Nota

STP sólo considera las interfaces operativas. Las interfaces que fallan (por ejemplo, interfaces sin cable instalado) o las interfaces administrativamente cerradas se colocan en estado Deshabilitado de STP. Así, esta sección utiliza el término **puertos operativos** para referirse a las interfaces que podrían enviar tramas si STP las coloca en estado de Envío.

La ID de puente STP y la BPDU Hello

El Algoritmo de árbol de extensión (STA) comienza con la elección de un switch para ser el switch raíz. Para comprender mejor este proceso de elección, se necesita entender los mensajes STP que se intercambian los switches, así como el concepto y formato del identificador utilizado para identificar de forma única cada switch.

El ID de puente (BID, *bridge ID*) de STP es un valor único de 8 bytes para cada switch. El ID de puente consta de un campo de prioridad de 2 bytes y un ID de sistema de 6 bytes, con el ID de sistema basado en una dirección MAC grabada en cada switch. El uso de una dirección MAC grabada asegura que cada ID de puente del switch será único.

STP define mensajes llamados *Unidades de datos del protocolo de puente* (BPDU *Bridge Protocol Data Units*), que utilizan los puentes y switches para intercambiar información entre ellos. El mensaje más común, llamado BPDU Hello, contiene el ID de puente del switch emisor. Indicando su propio y único ID de puente, los switches pueden diferenciar BPDUs enviadas desde diferentes switches. Este mensaje también contiene el ID de puente del switch raíz actual.

STP define varios tipos de mensajes BPDU, con la BPDU Hello como mensaje que realiza la mayoría del trabajo. La BPDU Hello incluye varios campos, los más importantes de los cuales se listan en la Tabla 2.4.

Tema clave **Tabla 2.4.** Campos de la BPDU Hello de STP.

Campo	Descripción
ID del puente raíz	El ID de puente del puente/switch que el remitente de este mensaje Hello cree que es el switch raíz.
ID del puente emisor	El ID de puente del puente/switch remitente de esta BPDU Hello.
Coste para alcanzar la raíz	El coste STP entre este switch y la raíz actual.
Valor de los temporizadores en el switch raíz	Incluye el temporizador Hello, el temporizador de Edad máxima (*MaxAge*) y el temporizador de Retardo de Envío (*Forward Delay*).

De momento, tenga en mente sólo los tres primeros elementos de la Tabla 2.4; las siguientes secciones se centran en los tres pasos de cómo STP elige las interfaces que entrarán en un estado de Envío. Después, el texto examina los tres principales pasos del proceso de STP.

Elección del switch raíz

Los switches eligen un switch raíz basándose en el ID de puente de las BPDUs. El switch raíz es el switch con el ID de puente de menor valor numérico. Ya que el ID de puente de dos partes comienza con el valor de prioridad, esencialmente el switch con la menor prioridad llega a ser la raíz. Por ejemplo, si uno de los switches tiene prioridad 100, y otro switch tiene prioridad 200, el switch con prioridad 100 gana, independientemente de qué dirección MAC se utilizara para crear el ID de puente para cada puente/switch.

Si basándose en la porción de prioridad del ID de puente se produce un empate, el switch con la menor dirección MAC en la parte del ID de puente es la raíz. No será necesaria ninguna otra forma de romper el empate porque los switches utilizan sus propias direcciones MAC grabadas como la segunda parte de sus ID de puente. Así, si hay empate de prioridades, y un switch utiliza la dirección MAC 0020.0000.0000 como parte del ID de puente, y el otro utiliza 0FFF.FFFF.FFF, el primero (MAC 0200.0000.0000) llega a ser la raíz.

STP elige un switch raíz de una manera no muy distinta a una elección política. El proceso comienza con todos los switches demandando ser la raíz mediante el envío de BPDUs Hello conteniendo su propio ID de puente como el ID de puente raíz. Si un switch escucha un mensaje Hello que contiene un mejor (más bajo) ID de puente (llamado Hello superior) ese switch finaliza las publicaciones de sí mismo como raíz y comienza a enviar el Hello superior. El Hello enviado por el mejor switch contiene el ID de puente del mejor switch como la raíz. Trabaja como una carrera política en la cual el candidato menos popular se rinde y deja la carrera, dando su apoyo a otro candidato. Finalmente, cualquiera está de acuerdo con el switch que tiene el mejor (más bajo) ID de puente, y todos apoyan al switch elegido (que es donde la analogía de la carrera política se cae en pedazos).

La Figura 2.3 muestra el comienzo del proceso de elección de la raíz. En este caso, SW1 se ha publicado a sí mismo como raíz, igual que SW2 y SW3. Sin embargo, SW2 cree ahora que SW1 es una mejor raíz, de modo que SW2 está ahora enviando el Hello originado en SW1. Este Hello reenviado contiene el BID de SW1 como el BID raíz. Sin embargo, en este punto, tanto SW1 como SW3 creen que cada uno de ellos es el mejor; por tanto, ellos todavía publican sus propios BIDs como la raíz en sus BPDUs Hello.

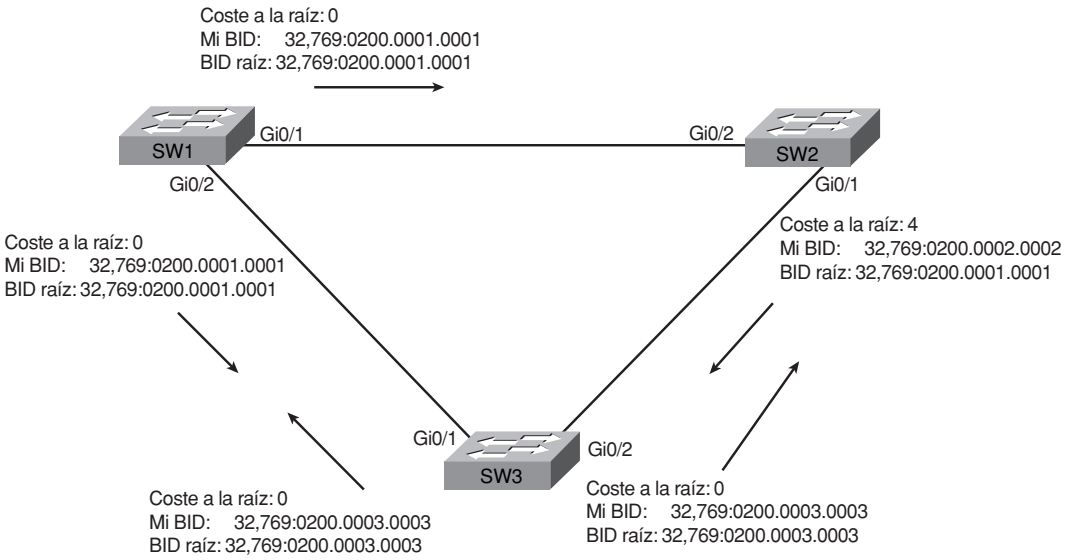


Figura 2.3. Los principios del proceso de elección de la raíz.

En la Figura 2.3 existen todavía dos candidatos: SW1 y SW3. Por tanto, ¿quién gana? Bien, del ID de puente, el switch de menor prioridad gana; si ocurre un empate, la menor dirección MAC gana. Como se muestra en la figura, SW1 tiene un menor ID de puente (32769:0200.0000.0001) que SW3 (32769:0200.0003.0003); por tanto, SW1 gana, y SW3 también cree ahora que SW1 es el mejor switch. La Figura 2.4 muestra los mensajes Hello resultantes enviados por los switches.

Una vez completa la elección, sólo el switch raíz continúa originando mensajes BPDU Hello de STP. Los otros switches reciben los Hello, actualizando el campo BID del remitente (y el campo de coste para alcanzar la raíz), y enviando los Hello por otras interfaces. La figura refleja este hecho, con SW1 enviando Hello en el Paso 1, y SW2 y SW3 enviando independientemente el Hello por sus otras interfaces en el Paso 2.

Elección del puerto raíz de cada switch

La segunda parte del proceso de STP tiene lugar cuando cada switch no raíz elige uno y sólo un **puerto raíz**. El puerto raíz de un switch (RP) es la interfaz a través de la cual tiene el menor coste de STP para alcanzar el switch raíz.

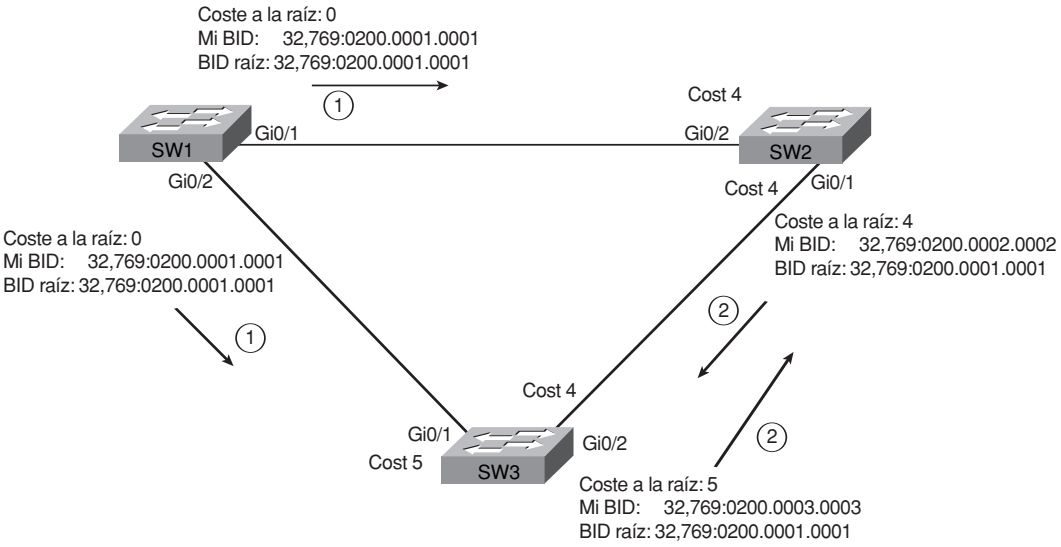


Figura 2.4. SW1 gana la elección.

Para calcular el coste, un switch añade el coste contenido en un Hello recibido al coste del puerto STP asignado a la misma interfaz. El coste del puerto STP es simplemente un valor asignado a cada interfaz con el propósito de proporcionar una medida objetiva que permita a STP seleccionar qué interfaces añadir a la topología de STP.

La Figura 2.5 muestra un ejemplo de cómo SW3 calcula su coste para alcanzar la raíz por los dos posibles caminos sumando el coste publicado (en los mensajes Hello) al coste de la interfaz mostrado en la figura.

Como resultado del proceso dibujado en la Figura 2.5, SW3 elige Gi0/1 como su RP, porque el coste para alcanzar el switch raíz a través de este puerto (5) es menor que la otra alternativa (Gi0/2, coste 8). De manera similar, SW2 elegirá Gi0/2 como su RP, con un coste de 4 (el coste publicado por SW1 de 0 más el coste de la interfaz Gi0/2 de SW2 de 4). Cada switch coloca sus puertos raíz en estado de Envío.

En topologías más complejas, la elección del puerto raíz puede no ser tan obvia. La sección "Resolución de problemas de STP", más adelante en este capítulo, muestra un ejemplo en el cual la elección del puerto raíz requiere pensarla un poco más.

Elección del puerto designado en cada segmento de LAN

El paso final de STP para elegir su topología es seleccionar el puerto designado en cada segmento de LAN. El puerto designado en cada segmento de LAN es el puerto del switch que publica el Hello de menor coste en un segmento de una LAN. Cuando un switch no raíz reenvía un Hello, el switch no raíz establece el campo de coste en el Hello al coste para

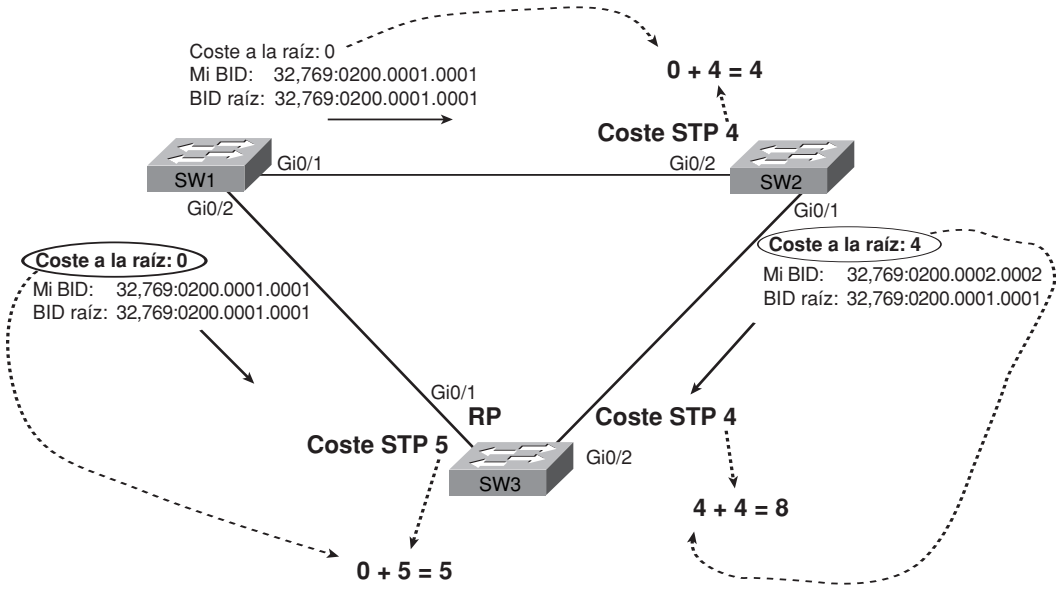


Figura 2.5. SW3 calculando el coste para alcanzar la raíz y seleccionando su RP.

alcanzar la raíz. En efecto, el switch con el menor coste para alcanzar la raíz, de entre todos los switches conectados a un segmento, llega a ser el DP en ese segmento.

Por ejemplo, en la Figura 2.4, SW2 y SW3 reenvían los mensajes Hello en el segmento. Obsérvese que SW2 y SW3 listan sus respectivos costes para alcanzar el switch raíz (coste 4 en SW2 y coste 5 en SW3). Como resultado, el puerto Gi0/1 de SW2 es el puerto designado en ese segmento de LAN.

Todos los DPs se colocan en estado de Envío; así en este caso, la interfaz Gi0/1 de SW2 pasará a un estado de reenvío.

Si existe empate en las publicaciones de coste, los switches rompen el empate seleccionando el switch con el menor ID de puente. En este caso, SW2 podría haber ganado, con un ID de puente de 32769:0200.0002.0002 frente a SW3 con 32769:0200.0003.0003.

Nota

Un switch puede conectar dos o más interfaces al mismo dominio de colisión si se utilizan hubs. En estos casos, se necesita otro criterio para romper el empate: el switch selecciona la interfaz con menor número interno de interfaz.

La única interfaz que no tiene razones para estar en un estado de Envío en los tres switches del ejemplo mostrados en las Figuras 2.3, 2.4 y 2.5 es el puerto Gi0/2 de SW3. Por tanto, el proceso de STP se ha completado. La Tabla 2.5 esboza el estado de cada puerto y por qué está en ese estado.

Los costes de puerto pueden ser configurados, o utilizar los valores predeterminados. La Tabla 2.6 muestra los costes de puerto predeterminados definidos por el IEEE; Cisco

Tabla 2.5. Estado de cada interfaz.

Switch, interfaz	Estado	Razón por la que la interfaz está en estado de Reenvío
SW1, Gi0/1	Envío	La interfaz está en el switch raíz.
SW1, Gi0/2	Envío	La interfaz está en el switch raíz.
SW2, Gi0/2	Envío	El puerto raíz.
SW2, Gi0/1	Envío	El puerto designado en el segmento de LAN para SW3.
SW3, Gi0/1	Envío	El puerto raíz.
SW3, Gi0/2	Bloqueo	No es puerto raíz y no es puerto designado.

Tabla 2.6. Costes de puerto predeterminados por el IEEE.

Velocidad Ethernet	Coste IEEE original	Coste IEEE Revisado
10 Mbps	100	100
100 Mbps	10	19
1 Gbps	1	4
10 Gbps	1	2

utiliza estos mismos valores. El IEEE revisó los valores de coste porque los valores originales, establecidos en los primeros años de los 80, no anticipaban el crecimiento de Ethernet para soportar 10 Gigabits.

Cuando se habilita STP, todas las interfaces operativas del switch establecerán un estado de Envío o de Bloqueo de STP, incluso los puertos de acceso. Para interfaces de switch conectadas a elementos o routers, que no utilizan STP, el switch enviará todavía Hellos por estas interfaces. Por la virtud de ser el único dispositivo enviando Hellos en ese segmento de LAN, el switch está enviando el Hello de coste mínimo en ese segmento de LAN, haciendo que el switch llegue a ser el puerto designado de ese segmento de LAN. Así, STP coloca a las interfaces de acceso que funcionan en un estado de Envío como resultado de la parte de puerto designado del proceso STP.

Cómo reaccionar frente a cambios en la red

Una vez determinada la topología de STP (el conjunto de interfaces en estado de reenvío), este conjunto de interfaces no cambia a menos que cambie la topología de la red. Esta sección examina el funcionamiento continuado de STP mientras la red está estable, y después examina cómo STP converge a una nueva topología cuando algo cambia.

El switch raíz envía una nueva BPDU Hello cada 2 segundos (valor predeterminado). Cada switch reenvía el Hello por todos los DPs, pero sólo después de cambiar dos elementos. Se cambia el valor del coste para reflejar el coste del switch para alcanzar la raíz, y el campo de ID de puente del remitente. (El campo de ID de puente de la raíz no cambia.) Al enviar los Hellos recibidos (y cambiados) por todos los DPs, todos los switches continúan recibiendo Hellos cada 2 segundos. La lista siguiente resume el funcionamiento sostenido cuando nada cambia en la topología de STP:

1. La raíz crea y envía una BPDU Hello, con un coste de 0, por todas sus interfaces operativas (aquellas en estado de Envío).
2. Los switches no raíces reciben el Hello en sus puertos raíz. Después de cambiar el Hello para listar su propio ID de puente como BID del remitente, y listando el coste a la raíz del switch, el switch reenvía el Hello por todos los puertos designados.
3. Repetir los Pasos 1 y 2 hasta que algo cambie.

Cada switch confía en estos mensajes Hello periódicos recibidos desde la raíz como una manera de conocer que su camino a la raíz está todavía funcionando. Cuando un switch cesa de recibir los Hellos, algo ha fallado; por tanto, el switch reacciona y comienza el proceso de cambio de topología del árbol de extensión. Por varias razones, el proceso de convergencia requiere el uso de tres temporizadores. Observe que todos los switches utilizan los temporizadores como dicta el switch raíz, temporizadores que la raíz incluye en sus mensajes BPDU Hello periódicos. Los temporizadores y sus descripciones se muestran en la Tabla 2.7.

Tabla 2.7. Temporizadores STP.

Temporizador	Descripción	Valor Predeterminado
Hello	Periodo de tiempo entre Hellos creados por la raíz.	2 segundos
Edad máxima	Cuánto debería esperar cualquier switch, después de no escuchar ya Hellos, antes de tratar de cambiar la topología de STP.	Hello 10 veces
Retardo de envío	Retardo que afecta al proceso que ocurre cuando una interfaz cambia de estado de Bloqueo a estado de Envío. Un puerto permanece en un estado de Escucha provisional, durante el número de segundos definido por el temporizador de retardo de reenvío.	15 segundos

Si un switch no recibe una esperada BPDU Hello en el tiempo Hello, el switch continúa normalmente. Sin embargo, si los Hellos no se presentan en el tiempo de Edad máxima, el switch reacciona realizando los pasos para cambiar la topología de STP. En este punto, el switch reevalúa qué switch podría ser el switch raíz, y si no es la raíz, qué puerto podría

ser su RP, y qué puertos podrían ser DPs, asumiendo que los Hellos que fueron anteriormente recibidos han dejado de llegar.

La mejor forma de describir la convergencia de STP es con un ejemplo que utilice alguna topología familiar. La Figura 2.6 muestra la misma figura ya familiar, con la interfaz Gi0/2 de SW3 en estado de Bloqueo, pero la interfaz Gi0/2 de SW1 acaba de fallar.

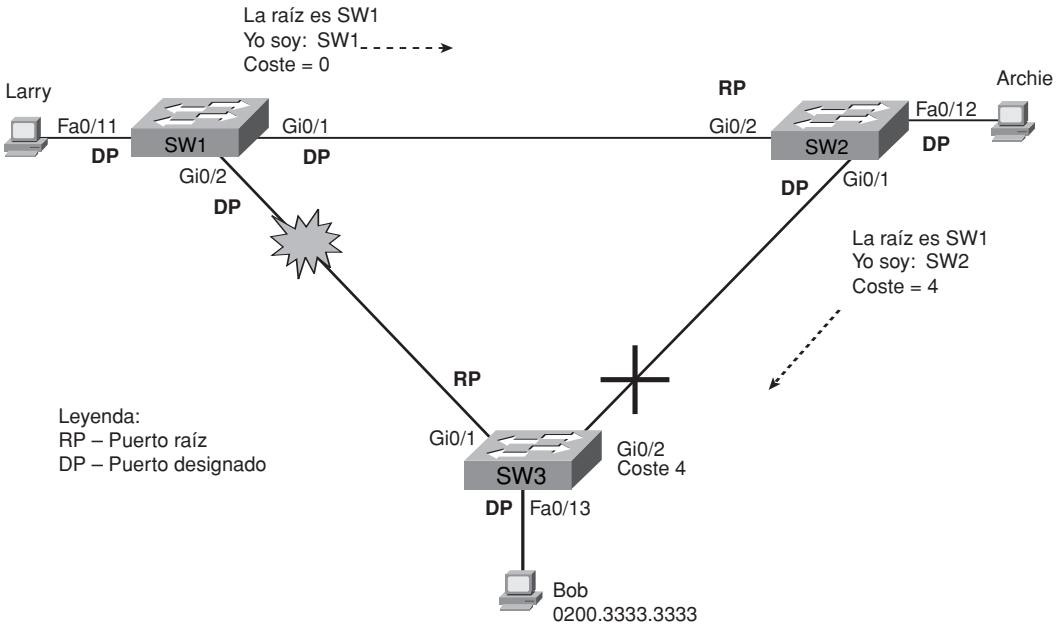


Figura 2.6. Reaccionando al fallo de un enlace entre SW1 y SW3.

SW3 reacciona al cambio porque deja de recibir sus esperados Hellos por su interfaz Gi0/1. Sin embargo, SW2 no necesita reaccionar porque continúa recibiendo sus Hellos periódicos por su interfaz Gi0/2. En este caso, SW3 reacciona cuando pasa el tiempo de Edad máxima sin escuchar los Hellos, o tan pronto como advierta que la interfaz Gi0/1 ha fallado. (Si la interfaz falla, el switch puede asumir que los Hellos ya no llegarán.)

Ahora que SW3 puede actuar, comienza por reevaluar la elección de un switch raíz. SW3 todavía recibe Hellos de SW1, reenviados por SW2, y SW1 tiene un ID de puente menor; por otra parte, SW1 ya no habría sido la raíz. Por tanto, SW3 decide que SW1 es todavía el mejor switch y que SW3 no es la raíz.

Después, SW3 reevalúa su selección de RP. En este punto, SW3 está sólo recibiendo Hellos por una interfaz, la interfaz Gi0/2. Calculando el coste, Gi0/2 llegará a ser el nuevo RP de SW3. (El coste sería 8: el coste publicado de SW2 4 más el coste de la interfaz Gi0/2,4.)

SW3 reevalúa entonces su rol como DP en todas las demás interfaces. En este ejemplo, no se necesita hacer un trabajo real. SW3 ya tenía un DP en la interfaz Fa0/13, y ésta continúa siendo el DP, porque no hay ningún otro switch conectado a ese puerto.

Cuando STP converge, un switch selecciona las interfaces que deben pasar de un estado a otro. Sin embargo, una transición de bloqueo a reenvío no puede ser realizada inmediatamente porque un cambio inmediato a reenvío podría causar que las tramas formaran bucles temporalmente. Para prevenir estos bucles temporales, en las transiciones STP, la interfaz pasa por dos estados intermedios, que son:

- **Escucha (*Listening*)**: Igual que en el estado de Bloqueo, la interfaz no reenvía tramas. Las entradas antiguas e incorrectas de la tabla MAC han caducado durante este estado, debido a que dichas entradas podrían provocar bucles temporales.
- **Aprendizaje (*Learning*)**: Las interfaces en este estado todavía no envían tramas, pero el switch comienza a aprender direcciones MAC de tramas recibidas por la interfaz.

STP cambia una interfaz de Bloqueo a Escucha, después a Aprendizaje, y después al estado de Envío. STP deja la interfaz en cada uno de estos estados interinos por un tiempo igual al del temporizador de retardo de reenvío. Como resultado, un evento de convergencia que causa el cambio de una interfaz de Bloqueo a Envío necesita 30 segundos para la transición de Bloqueo a Envío. Además, un switch podría tener que esperar los segundos de Edad máxima antes incluso de decidir mover una interfaz del estado de Bloqueo al de Envío. Siguiendo con el mismo ejemplo mostrado en las últimas figuras, SW3 debe esperar los segundos de Edad máxima antes de decidir que no volverá a recibir la misma BPDU raíz por su puerto raíz (20 segundos es el valor predeterminado), y entonces esperar 15 segundos en cada estado de Escucha y Aprendizaje en su interfaz Gi0/2, resultando un retardo de convergencia de 50 segundos.

La Tabla 2.8 resume varios de los estados de las interfaces del Árbol de extensión para una fácil revisión.

Tabla 2.8. Estados del Árbol de extensión del IEEE 802.1d.

Estado	¿Reenvía tramas de datos?	¿Aprende MACs básandose en las tramas recibidas?	¿Estado transitorio o estable?
Bloqueo	No	No	Estable
Escucha	No	No	Transitorio
Aprendizaje	No	Sí	Transitorio
Envío	Sí	Sí	Estable
Deshabilitado	No	No	Estable

Características opcionales de STP

STP tiene más de 20 años. Los switches de Cisco implementan el estándar STP IEEE 802.1d, pero durante estos años, Cisco ha añadido características propietarias para intro-

ducir mejoras en STP. En algunos casos, el IEEE ha añadido estas mejoras, o algunas parecidas, a sus estándares posteriores, como una revisión del estándar o como un estándar adicional. Las siguientes secciones examinan tres de los añadidos propietarios a STP: EtherChannel, PortFast, y BPDU Guard.

NOTA

Si se plantea trabajar en una LAN de campus de producción, probablemente necesite aprender más sobre las características de STP que las tratadas en este libro. Para hacer esto, consulte la Guía de configuración de software de Cisco para los switches 2960 y busque los capítulos de STP, RSTP y características opcionales de STP. La introducción de este libro tiene información de cómo obtener documentación de Cisco.

EtherChannel

Una de las mejores maneras de disminuir el tiempo de convergencia de STP es evitar la convergencia completamente. EtherChannel proporciona una forma de prevenir la necesidad de la convergencia de STP cuando sólo ocurre un fallo en un único puerto o cable.

EtherChannel combina segmentos paralelos múltiples de igual velocidad (hasta ocho) entre el mismo par de switches, unidos en un EtherChannel. Los switches tratan al EtherChannel como una única interfaz a considerar en el proceso de reenvío de tramas y para STP. Como resultado, si uno de los enlaces falla, pero al menos uno de ellos está operativo, la convergencia de STP no tiene que ocurrir. Por ejemplo, la Figura 2.7 muestra la familiar red de tres switches, pero ahora con dos conexiones Gigabit Ethernet entre cada par de switches.

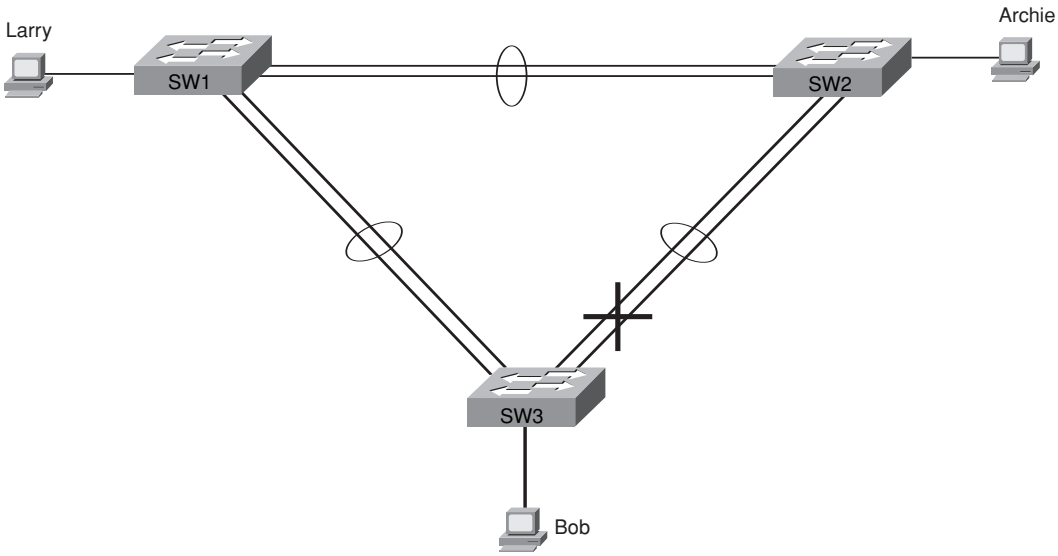


Figura 2.7. Dos segmentos EtherChannels entre switches.

Con cada par de enlaces Ethernet configurados como un EtherChannel, STP trata cada EtherChannel como un único enlace. En otras palabras, deben fallar ambos enlaces con el mismo switch para que el switch tenga que provocar la convergencia de STP. Sin EtherChannel, si se tienen enlaces paralelos múltiples entre dos switches, STP bloquea todos los enlaces excepto uno. Con EtherChannel, todos los enlaces paralelos pueden estar activos y funcionando al mismo tiempo, lo que aumenta la disponibilidad de la red, mientras se reduce el número de veces que STP debe converger.

EtherChannel proporciona también mayor ancho de banda de red. Todos los troncales en un EtherChannel están o reenviando o bloqueados, porque STP trata a todos los troncales en el mismo EtherChannel como un único troncal. Cuando un EtherChannel está en estado de Envío, los switches equilibran la carga de tráfico entre todos los troncales, proporcionando mayor ancho de banda.

PortFast

PortFast permite al switch colocar inmediatamente un puerto en estado de Envío cuando el puerto se activa físicamente, ignorando cualquier opción sobre la topología de STP e ignorando los estados de Escucha y Aprendizaje. Sin embargo, los únicos puertos en los que se puede habilitar PortFast de forma segura son aquellos que no conectan con puentes, switches, o cualquier otro dispositivo que hable STP.

PortFast es más apropiado para conexiones de dispositivos de usuario final. Si se establece PortFast en puertos conectados a dispositivos de usuario final, cuando el PC de un usuario final arranca, tan pronto como la NIC del PC se activa, el puerto del switch puede pasar al estado de Envío de STP y reenviar tráfico. Sin PortFast, cada puerto debe esperar mientras el switch confirma que el puerto es un DP, y entonces espera mientras la interfaz pasa por los estados temporales de Escucha y Aprendizaje antes de establecer el estado de Envío.

Seguridad en STP

Las interfaces de un switch que conectan localizaciones de usuario final en la LAN tienen algunas exposiciones de seguridad. Un atacante podría conectar un switch a uno de estos puertos, con un valor de prioridad de STP bajo, y llegar a ser el switch raíz. También, conectando un switch pirata a múltiples switches legítimos, el switch pirata podría terminar reenviando mucho tráfico en la LAN, y el atacante podría utilizar un analizador de LAN para copiar un gran número de tramas de datos enviadas a través de esa LAN. También, los usuarios podrían dañar inocentemente la LAN. Por ejemplo, un usuario podría comprar y conectar un switch LAN barato de consumidor a otro switch existente, posiblemente creando un bucle, o posiblemente provocando que el nuevo switch de potencia relativamente baja llegue a ser la raíz.

La característica de BPDU Guard de Cisco ayuda a evitar esta clase de problemas deshabilitando un puerto si se recibe por él una BPDU. Así, esta característica es particularmente útil en puertos que sólo se utilizarán como puerto de acceso y nunca conectados a

otro switch. Además, la característica BPDU Guard se utiliza a menudo en la misma interfaz que tiene habilitado PortFast, ya que un puerto con PortFast habilitado estará ya en un estado de Envío, lo que incrementa la posibilidad de bucles de envío.

La característica Cisco Root Guard ayuda a evitar el problema cuando el nuevo y pícaro switch trata de llegar a ser el switch raíz. La prestación Root Guard permite que se pueda conectar a la interfaz otro switch, y participar en STP enviando y recibiendo BPDUs. Sin embargo, cuando la interfaz del switch con Root Guard habilitado recibe una BPDU superior del switch vecino (una BPDU con un ID de puente menor/mejor) el switch con Root Guard reacciona. No sólo ignora la BPDU superior, sino que el switch también deshabilita la interfaz, no enviando ni recibiendo tramas, mientras las BPDUs superiores sigan llegando. Si las BPDUs superiores dejan de llegar, el switch puede comenzar de nuevo a utilizar la interfaz.

STP Rápido (IEEE 802.1w)

Como se ha mencionado anteriormente en este capítulo, el IEEE define STP en el estándar IEEE 802.1d. El IEEE ha mejorado el protocolo 802.1d con la definición del Protocolo de árbol de extensión rápido (RSTP, *Rapid Spanning Tree Protocol*), definido en el estándar 802.1w.

RSTP (802.1w) funciona exactamente igual a STP (802.1d) en varios aspectos:

- Elige un switch raíz utilizando los mismos parámetros y criterios para deshacer los empates.
- Elige el puerto raíz en los switches no raíces con las mismas reglas.
- Elige los puertos designados en cada segmento LAN con las mismas reglas.
- Coloca cada puerto en el estado de Envío o de Bloqueo, aunque RSTP denomina al estado de Bloqueo el estado de Descarte.

RSTP puede desplegarse junto al tradicional STP 802.1d, con las características de RSTP funcionando en switches que la soporten, y las características del tradicional STP 802.1d funcionando en los switches que únicamente soporten STP.

Con todas estas semejanzas, en primer lugar podríamos preguntarnos por qué el IEEE se molestó en crear RSTP. La razón que prima es la convergencia. STP tarda un tiempo relativamente largo en converger (50 segundos con los valores predeterminados). RSTP mejora la convergencia de la red cuando se producen cambios en la topología.

RSTP mejora la convergencia bien eliminando o bien reduciendo significativamente los periodos de espera que STP 802.1d necesita para evitar bucles durante la convergencia. STP 802.1d necesita un periodo de espera de Edad máxima (con un valor predeterminado de 20 segundos) antes de reaccionar ante algunos eventos, mientras que RSTP sólo tiene que esperar 3*Hello (6 segundos de forma predeterminada). Además, RSTP elimina el tiempo de retardo de envío (valor predeterminado de 15 segundos) en los estados de Escucha y Aprendizaje. La convergencia del tradicional STP tiene esencialmente tres periodos de tiempo, cada uno de los cuales RSTP mejora. Es-

tos tres periodos de espera de 20, 15 y 15 segundos (valor predeterminado) conllevan una convergencia relativamente lenta de STP 802.1d, y la reducción o eliminación de estos periodos de espera hace que la convergencia de RSTP ocurra más rápidamente.

Los tiempos de convergencia de RSTP son típicamente inferiores a 10 segundos. En algunos casos, pueden ser tan bajos como 1 ó 2 segundos. Las siguientes secciones explican la terminología y los procesos utilizados por RSTP para superar las limitaciones de STP 802.1d y mejorar el tiempo de convergencia.

Nota

Al igual que la mayoría de los textos, cuando sea necesario distinguir entre los estándares 802.1d antiguo y 802.1w nuevo, STP se refiere a 802.1d, y RSTP se refiere a 802.1w.

Tipos de enlace y contorno RSTP

RSTP caracteriza los tipos de conectividad física en una LAN de campus en tres tipos diferentes:

- Tipo de enlace punto a punto.
- Tipo de enlace compartido.
- Tipo de contorno (*edge-type*).

La Figura 2.8 muestra cada tipo.

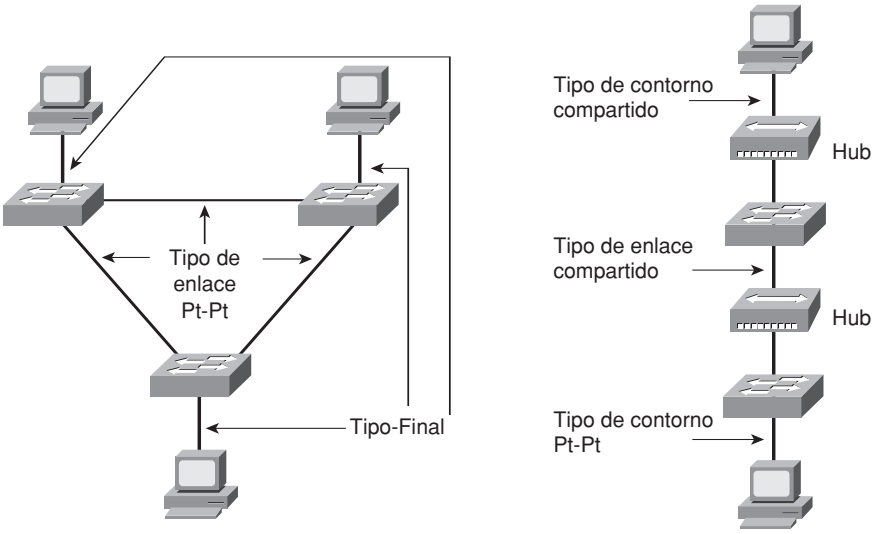


Figura 2.8. Tipos de enlace y contorno RSTP.

La Figura 2.8 muestra dos ejemplos de redes. La red de la izquierda es un diseño actual típico de campus, sin hubs. Todos los switches y todos los dispositivos de usuario final están conectados con cables Ethernet. El IEEE definió RSTP para mejorar la convergencia en este tipo de redes.

En la red de la parte derecha de la figura, todavía se utilizan hubs para las conexiones entre switches, así como para las conexiones de dispositivos de usuario final. La mayoría de las redes ya no usan hubs. El IEEE no trata de hacer que RSTP trabaje en esas redes que utilizan hubs compartidos, y RSTP no mejorará la convergencia en la red de la derecha.

RSTP llama a las conexiones Ethernet entre switches **enlaces** y a las conexiones Ethernet con dispositivos de usuario final **contornos**. Existen dos tipos de enlaces: punto a punto, como se muestra en el lado izquierdo de la Figura 2.8, y compartido, como puede verse en el lado derecho. RSTP no diferencia entre los tipos punto a punto y compartido para las conexiones de contorno.

RSTP reduce el tiempo de convergencia para las conexiones de tipo de enlace punto a punto y de tipo contorno. No mejora la convergencia sobre conexiones de tipo de enlace compartido. Sin embargo, la mayoría de las redes modernas no utilizan hubs entre switches; por tanto, la falta de mejoras en la convergencia de RSTP para el tipo de enlace compartido realmente no importa.

Estados de puerto RSTP

También se debe estar familiarizado con los nuevos términos de RSTP para describir un estado de puerto. La Tabla 2.9 especifica estos estados, con alguna explicación a continuación de la tabla.

Tema clave

Tabla 2.9. Estados de puerto de RSTP y STP.

Estado operativo	Estado STP (802.1d)	Estado RSTP (802.1W)	¿Envía tramas de datos en este estado?
Habilitado	Bloqueo	Descarte	No
Habilitado	Escucha	Descarte	No
Habilitado	Aprendizaje	Aprendizaje	No
Habilitado	Envío	Envío	Sí
Deshabilitado	Deshabilitado	Descarte	No

De forma similar a STP, RSTP estabiliza todos los puertos bien al estado de Envío o bien al estado de Descarte. **Descarte** significa que el puerto no envía tramas, procesa tramas recibidas, o aprende direcciones MAC; pero escucha BPDUs. Para abreviar, actúa exactamente igual que el estado de Bloqueo de STP. RSTP utiliza un estado de Aprendizaje interino cuan-

do cambia una interfaz desde el estado de Descarte al estado de Envío. Sin embargo, RSTP necesita utilizar el estado de Aprendizaje sólo durante un tiempo corto.

Roles de puerto RSTP

Ambos, STP (802.1d) y RSTP (802.1w), utilizan los conceptos de estados y roles de puerto. El proceso de STP determina el rol de cada interfaz. Por ejemplo, STP determina qué interfaces tienen actualmente el rol de puerto raíz y puerto designado. Entonces, STP determina el estado estable de puerto a utilizar para las interfaces en ciertos roles: el estado de Envío para puertos en los roles RP o DP, y el estado de Bloqueo para puertos en otros roles.

RSTP añade tres roles de puerto más, dos de los cuales se muestran en la Figura 2.9. (El tercer rol, el rol deshabilitado, no se muestra en la figura; se refiere simplemente a interfaces cerradas.)

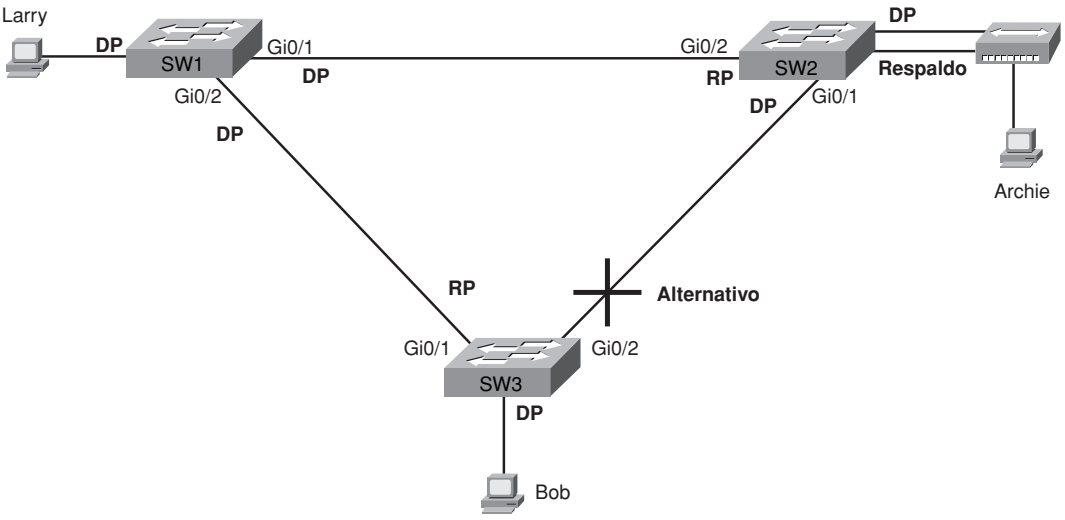


Figura 2.9. Roles de puerto en RSTP.

El rol de puerto **alternativo** de RSTP identifica al mejor switch alternativo para su actual RP. Para abreviar, el rol de puerto alternativo es un RP alternativo. Por ejemplo, SW3 tiene a Gi0/1 como su RP, pero SW3 también conoce que está recibiendo BPDUs Hello por la interfaz Gi0/2. El switch SW3 tiene un puerto raíz, igual que lo tendría con STP. (La Figura 2.4 repasa el flujo de estados estables de BPDUs.) RSTP designa los puertos que reciben BPDUs subóptimas (BPDUs que no son tan "buenas" como las recibidas por el puerto raíz) como puertos alternativos. Si SW3 deja de recibir Hellos del puente raíz, RSTP en SW3 elige el mejor puerto alternativo como su nuevo puerto raíz para comenzar el proceso de convergencia más rápido.

El otro nuevo tipo de puerto de RSTP, puerto de **respaldo**, se aplica sólo cuando un único switch tiene dos enlaces al mismo segmento (dominio de colisión). Para tener dos enlaces con el mismo dominio de colisión, el switch debe estar conectado a un hub, como se muestra en la Figura 2.9 en SW2. En la figura, el switch SW2 coloca uno de los dos puertos en el rol de puerto designado (y eventualmente en un estado de Envío) y la otra interfaz en el rol de respaldo (y eventualmente en el estado de Descarte). SW2 envía BPDUs por el puerto en estado Envío y toma la misma BPDU de respaldo por el puerto que está en estado de Descarte. Por tanto, SW2 conoce que tiene una conexión extra a ese segmento, llamado **puerto de respaldo**. Si el puerto DP en estado Envío falla, SW2 puede cambiar rápidamente ese puerto de respaldo del estado de Descarte al estado de Aprendizaje y después al estado de Envío.

La Tabla 2.10 muestra los roles de puerto para STP y RSTP.

Tema clave **Tabla 2.10.** Roles de puerto de STP y RSTP.

Rol RSTP	Rol STP	Definición
Puerto raíz	Puerto raíz	Un único puerto en cada switch no raíz en el cual el switch escucha la mejor BPDU de entre todas las recibidas.
Puerto designado	Puerto designado	De todos los puertos de switch en todos los switches conectados al mismo dominio de colisión/segmento, el puerto que publica la "mejor" BPDU.
Puerto alternativo	—	Un puerto en un switch que recibe una BPDU subóptima.
Puerto de respaldo	—	Un puerto no designado de un switch que está conectado al mismo segmento/dominio de colisión que otro puerto del mismo switch.
Deshabilitado	—	Un puerto que está administrativamente deshabilitado o no funciona por alguna otra razón.

Convergencia de RSTP

Esta sección de RSTP muestra lo parecidos que son RSTP y STP: cómo ambos eligen una raíz utilizando las mismas reglas, seleccionan los puertos designados usando las mismas reglas, y así sucesivamente. Si RSTP hiciera únicamente las mismas cosas que STP, no habría habido ninguna necesidad de actualizar el estándar original STP 802.1d con el nuevo estándar RSTP 802.1w. La principal razón para el nuevo estándar es mejorar el tiempo de convergencia.

El Algoritmo de árbol de extensión (STA, *Spanning Tree Algorithm*) de RSTP funciona algo diferente a su viejo predecesor. Por ejemplo, en condiciones estables, todo switch independientemente genera y envía BPDUs Hello, en lugar de sólo los cambios y reenvíos de Hellos enviados por el switch raíz. Sin embargo, en condiciones estables, el resultado

final es el mismo: un switch que continúa escuchando los mismos Hellos, con el mismo coste y BID raíz del switch, deja la topología STP como está.

El principal cambio con la versión RSTP de STA ocurre cuando se producen cambios en la red. RSTP actúa de forma diferente en la misma interfaz dependiendo de la caracterización de interfaces que realiza RSTP basada en qué está conectado a la interfaz.

Comportamiento de tipo contorno y PortFast

RSTP mejora la convergencia de las conexiones de tipo contorno colocando inmediatamente el puerto en estado de Envío cuando el enlace está físicamente activo. En efecto, RSTP trata estos puertos justo como lo hace la característica PortFast propietaria de Cisco. De hecho, en los switches de Cisco, para habilitar RSTP en interfaces de contorno, simplemente configure PortFast.

Tipo enlace compartido

RSTP no hace nada diferente a STP en los enlaces de tipo enlace compartido. Sin embargo, debido a que la mayoría de los enlaces actuales entre switches no son compartidos, normalmente son enlaces punto a punto dúplex, esto no importa.

Tipo enlace punto a punto

RSTP mejora la convergencia en enlaces dúplex entre switches (los enlaces que RSTP denomina "tipo enlace punto a punto"). La primera mejora introducida por RSTP en este tipo de enlaces está relacionada con cómo STP utiliza el temporizador de Edad máxima. STP necesita que un switch que no recibe BPDUs raíz por su puerto raíz espere los segundos de Edad máxima antes de iniciar la convergencia. El valor predeterminado de Edad máxima es de 20 segundos. RSTP reconoce la pérdida del camino hasta el puente raíz, a través del puerto raíz, en 3 veces el tiempo del temporizador Hello, o en 6 segundos con un valor predeterminado de 2 segundos del temporizador Hello. Así, RSTP reconoce un camino perdido hasta la raíz mucho más rápidamente.

RSTP elimina la necesidad del estado de Escucha y reduce el tiempo necesario para que el estado de Aprendizaje active el descubrimiento del nuevo estado de la red. STP espera pasivamente nuevas BPDUs y reacciona a ellas durante los estados de Escucha y Aprendizaje. Con RSTP, los switches negocian con los switches vecinos enviando mensajes de RSTP. Los mensajes permiten a los switches determinar rápidamente si una interfaz puede pasar inmediatamente a un estado de Envío. En la mayoría de los casos, el proceso tarda sólo un segundo o dos para el dominio de RSTP entero.

Ejemplo de convergencia rápida de RSTP

En lugar de explicar cada matiz de la convergencia de RSTP, un ejemplo puede aportarnos el conocimiento suficiente sobre el proceso. La Figura 2.10 muestra una red que explica la convergencia RSTP.

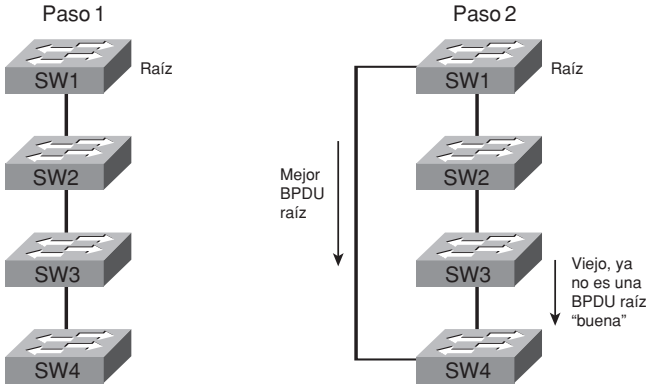


Figura 2.10. Ejemplo de convergencia de RSTP: Pasos 1 y 2.

La Figura 2.10 establece el problema. En la izquierda, en el Paso 1, la red no tiene redundancia. RSTP ha colocado todos los enlaces de tipo enlace punto a punto en estado Envío. Para añadir redundancia, los ingenieros de red añaden otro enlace de tipo enlace punto a punto entre SW1 y SW4, como se muestra a la derecha como Paso 2. Por tanto, es necesario que RSTP inicie la convergencia.

El primer paso de la convergencia tiene lugar cuando SW4 comprende que está recibiendo una BPDU mejor que la que estaba recibiendo de SW3. Como ambas, las BPDUs raíz nueva y vieja, publican el mismo switch, SW1, la nueva y "mejor" BPDU que llega por un enlace directo desde SW1 debe ser mejor por el menor coste. Independientemente de la razón, SW4 necesita realizar la transición al estado Envío en el nuevo enlace con SW1, porque es ahora el puerto raíz de SW4.

En este punto, el comportamiento de RSTP se aparte al de STP. RSTP en SW4 bloquea ahora temporalmente todos los otros puertos de tipo enlace. Haciendo esto, SW4 previene la posibilidad de introducir bucles. Entonces SW4 negocia con sus vecinos en el nuevo puerto raíz, SW1, usando mensajes de propuesta y acuerdo de RSTP. Como resultado, SW4 y SW1 acuerdan que cada uno puede colocar sus respectivos extremos del nuevo enlace en estado de Envío inmediatamente. La Figura 2.11 muestra este tercer paso.

¿Por qué SW1 y SW4 pueden colocar sus extremos del nuevo enlace en estado de Envío sin provocar bucles? Porque SW4 bloquea todos los otros puertos de tipo enlace. Dicho de otra forma, bloquea todos los otros puertos conectados a otros switches. Ésta es la clave para entender la convergencia de RSTP. Un switch sabe que necesita cambiar a un nuevo puerto raíz, bloquea todos los otros enlaces y después negocia el paso del nuevo puerto raíz a estado de Envío. Esencialmente, SW4 le dice a SW1 que confíe en él y comience a enviar, porque SW4 promete bloquear todos los otros puertos hasta estar seguro de que puede cambiar alguno de ellos de nuevo al estado de Envío.

Sin embargo, el proceso no está todavía completo. La topología RSTP actual muestra a SW4 bloqueado, que en este ejemplo no es la topología final mejor.

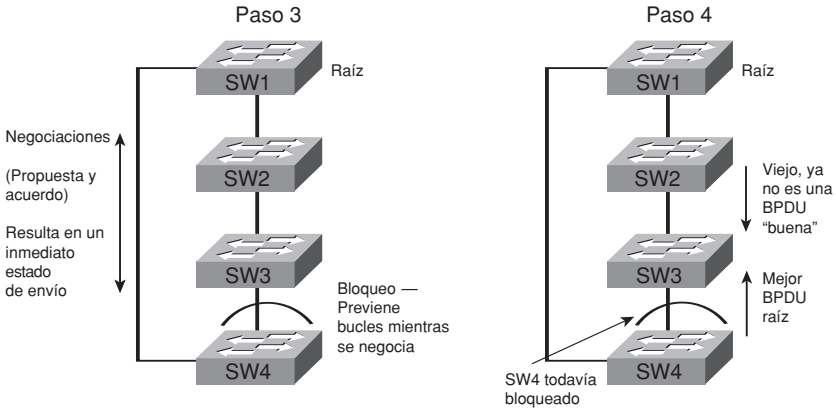


Figura 2.11. Ejemplo de convergencia de RSTP: Pasos 3 y 4 .

SW4 y SW3 repiten el mismo proceso que SW1 y SW4 acaban de realizar. En el Paso 4, SW4 todavía bloquea, previniendo bucles. Sin embargo, SW4 envía la nueva BPDU raíz a SW3; así, SW3 escucha ahora dos BPDUs. En este ejemplo, se asume que SW3 piensa que la BPDU de SW4 es mejor que la recibida de SW2; esto hace que SW3 repita el mismo proceso que SW4 acaba de realizar. A partir de este punto se sigue este flujo general:

1. SW3 decide cambiar su puente raíz basándose en esta nueva BPDU de SW4.
2. SW3 bloquea todos los otros puertos de tipo enlace. (RSTP denomina a este proceso **sincronización**.)
3. SW3 y SW4 negocian.
4. Como resultado de la negociación, SW4 y SW3 pueden pasar a enviar por sus interfaces de cualquier extremo del enlace de tipo enlace punto a punto.
5. SW3 mantiene el estado de Bloqueo en todos los demás puertos de tipo enlace hasta el siguiente paso en la lógica.

La Figura 2.12 muestra en la parte izquierda algunos de estos pasos del Paso 5 y la conducta resultante en el Paso 6.

SW3 todavía bloquea su interfaz superior en este punto. Observe que SW2 está ahora recibiendo dos BPDUs, pero la misma BPDU antigua que había estado recibiendo desde el principio es todavía la mejor BPDU. Así, SW2 no realiza ninguna acción. ¡Y RSTP ha acabado convergiendo!

Aunque la explicación ha ocupado varias páginas, el proceso de este ejemplo puede tardar menos de 1 segundo en completarse. Para los exámenes CCNA, debe recordar la terminología relativa a RSTP, así como el concepto de que RSTP mejora el tiempo de convergencia comparado con STP.

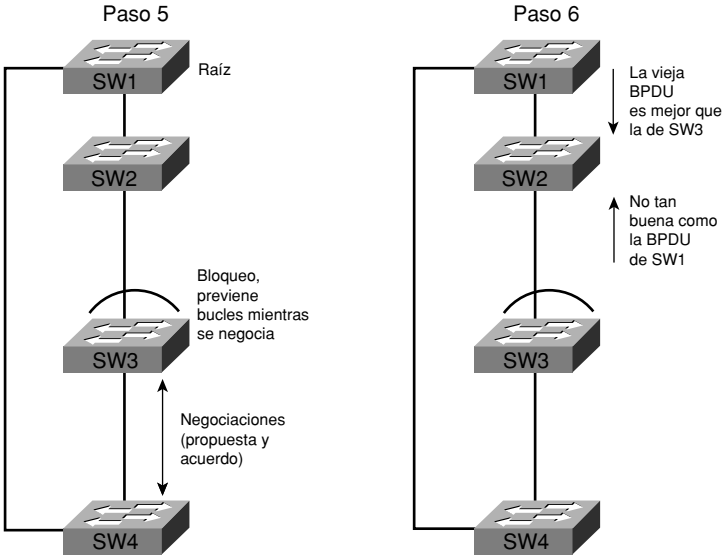


Figura 2.12. Ejemplo de convergencia RSTP: Pasos 5 y 6.

Configuración y verificación de STP

Los switches de Cisco utilizan STP (IEEE 802.1d) de forma predeterminada. Se pueden comprar algunos switches y conectarlos con cables Ethernet en una topología redundante, y STP garantizará la ausencia de bucles. ¡Y nunca habrá que pensar en cambiar ningún valor de configuración!

Aunque STP funciona sin ninguna configuración, es necesario entender cómo funciona STP, cómo interpretar los comandos show relativos a STP, y cómo poner a punto STP configurando varios parámetros. Por ejemplo, de forma predeterminada, todos los switches utilizan la misma prioridad; por tanto, el switch con menor dirección MAC grabada se convierte en la raíz. En cambio, un switch puede ser configurado con una menor prioridad, de modo que el ingeniero siempre conoce qué switch es la raíz, asumiendo que ese switch está activo y funcionando.

Las siguientes secciones comienzan describiendo algunas opciones para el equilibrado de la carga de tráfico asumiendo múltiples instancias de STP, seguidas por una corta descripción de cómo configurar STP para aprovechar las ventajas de esas múltiples instancias de STP. El resto de estas secciones muestran varios ejemplos de configuración de STP y RSTP.

Instancias múltiples de STP

Cuando el IEEE estandarizó STP, las VLANs aún no existían. Cuando más tarde se estandarizaron las VLANs, el IEEE no definió ningún estándar que permitiera más de una

instancia de STP, aun con múltiples VLANs. En ese momento, si un switch sólo seguía los estándares del IEEE, el switch aplicaba una instancia de STP en todas las VLANs. Dicho de otra forma, si una interfaz está enviando, lo hace para todas las VLANs, y si está bloqueada, de nuevo bloquea todas las VLANs.

De forma predeterminada, los switches de Cisco utilizan IEEE 802.1d, no RSTP (802.1w), con una característica propietaria de Cisco llamada Protocolo de árbol de extensión por VLAN Plus (PVST+, *Per-VLAN Spanning Tree Plus*). PVST+ (hoy abreviado simplemente como PVST) crea una instancia diferente de STP por cada VLAN. Así, antes de echar un vistazo a los parámetros de puesta a punto de STP, es necesario tener unos conocimientos básicos de PVST+, porque los valores de configuración pueden ser diferentes para cada instancia de STP.

PVST+ proporciona a los ingenieros una herramienta de equilibrado de la carga. Cambiando algunos parámetros de configuración de STP en diferentes VLANs, el ingeniero podría hacer que los switches tomaran diferentes RPs y DPs en distintas VLANs. Como resultado, el tráfico de unas VLANs puede ser enviado por un troncal, y el tráfico de otras ser enviado por un troncal diferente. La Figura 2.13 muestra la idea básica, con SW3 enviando el tráfico de las VLANs impares por el troncal de la izquierda (Gi0/1) y el de las VLANs pares por el de la derecha (Gi0/2).

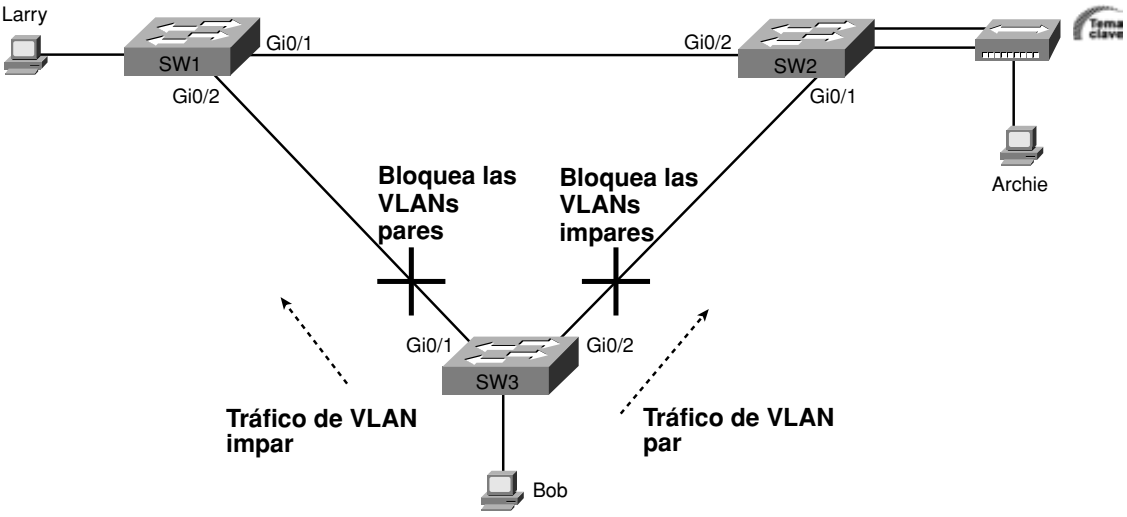


Figura 2.13. Equilibrado de la carga con PVST+.

Más tarde, cuando el IEEE introdujo RSTP 802.1W, el IEEE todavía no tenía un estándar para utilizar múltiples instancias de STP. Por tanto, Cisco implementó otra solución propietaria para soportar una VLAN por árbol de extensión de RSTP. Cisco ha llamado a esta opción Árbol de extensión por VLAN rápido (RPVST, *Rapid Per-VLAN Spanning Tree*) o Árbol de extensión rápido por VLAN (PVRST, *Per-VLAN Rapid Spanning Tree*). Independientemente del acrónimo, la idea es justo como en PVST+, pero aplicada a RSTP: una ins-

tancia de RSTP para controlar cada VLAN. Así, no sólo se consigue una convergencia más rápida, sino que también se puede equilibrar la carga como se muestra en la Figura 2.13.

Más tarde, el IEEE creó una opción estandarizada para múltiples árboles de extensión. El estándar de IEEE (802.1s) se denomina Árboles de extensión múltiples (MST, *Multiple Spanning Trees*) o Instancias múltiples de árboles de extensión (MIST, *Multiple Instances of Spannings Trees*). MIST permite la definición de instancias múltiples de RSTP, con cada VLAN asociada con una instancia particular. Por ejemplo, para conseguir el efecto de equilibrado de la carga en la Figura 2.13, MIST podría crear dos instancias de RSTP: una para las VLANs pares y otra para las impares. Si existen 100 VLANs, los switches sólo necesitarían dos instancias de RSTP, en lugar de las 100 instancias utilizadas por PVRST. Sin embargo, MIST necesita una mayor configuración en cada switch, principalmente para definir las instancias de RSTP y asociar cada VLAN con una instancia de STP.

La Tabla 2.11 resume estas tres opciones de múltiples árboles de extensión.

Tabla 2.11. Comparación de tres opciones para múltiples árboles de extensión.

Opción	Soporta STP	Soporta RSTP	Esfuerzo de configuración	Sólo es necesaria una instancia para cada ruta redundante
PVST+	Sí	No	Pequeño	No
PVRST+	No	Sí	Pequeño	No
MIST	No	Sí	Medio	Sí

Opciones de configuración que influyen en la topología del árbol de extensión

Con independencia de si se usa PVST+, PVRST o MIST, se pueden utilizar dos opciones principales de configuración para lograr el tipo de efectos de equilibrado de la carga descritos en torno a la Figura 2.13: el ID de puente y el coste de puerto. Estas opciones impactan en la topología de STP por VLAN como sigue:

- Los ID de puente influyen en la elección del switch raíz, y para los switches no raíces, eligen el puerto raíz.
- El coste STP (por VLAN) de cada interfaz para alcanzar la raíz, que influye en la elección de puerto designado en cada segmento de LAN.

Las siguientes secciones señalan algunos detalles particulares de la implementación de STP en los switches de Cisco, más allá de los conceptos genéricos ya tratados en este capítulo.

El ID de puente y la extensión del ID de sistema

Como ya se ha mencionado antes en este capítulo, el ID de puente de un switch (BID) está formado por la combinación de 2 bytes de prioridad y 6 bytes de la dirección MAC del

switch. En la práctica, los switches de Cisco utilizan un formato más detallado del BID del IEEE que separa la prioridad en dos partes. La Figura 2.14 muestra el formato más detallado, con el campo de 16 bits de prioridad incluyendo un subcampo de 12 bits llamado **extensión del ID de sistema**.

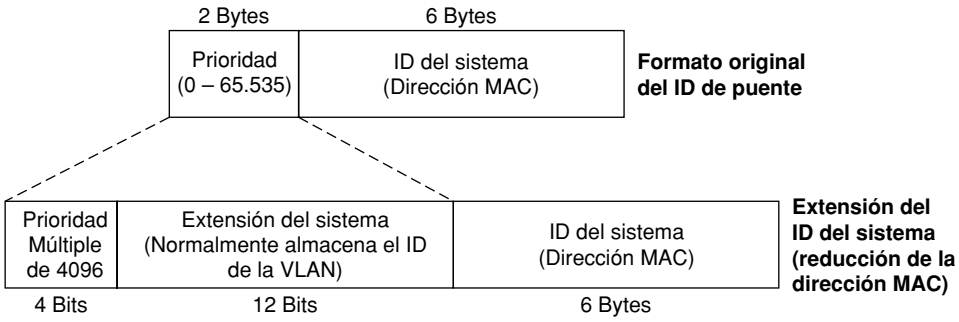


Figura 2.14. Extensión del ID del sistema STP.

Para crear el BID de un switch para una instancia de STP para una VLAN particular, el switch debe usar una prioridad base con un valor múltiplo del decimal 4096. (Los múltiplos de 4096, cuando se convierten a binario, acaban todos con 12 ceros binarios). Para asignar los primeros 16 bits del BID para una VLAN particular, el switch comienza con una versión de 16 bits del valor de prioridad básica, que tiene todo ceros binarios en los últimos 12 dígitos. El switch añade entonces a su valor de prioridad básica el ID de la VLAN. El resultado es que los 12 bits de menor orden en el campo original de prioridad contienen el ID de la VLAN.

Un buen efecto colateral de usar la extensión del ID del sistema es que PVST+ utiliza entonces un BID diferente para cada VLAN. Por ejemplo, un switch configurado con las VLANs 1 a 4, con una prioridad base predeterminada de 32.768, tiene una prioridad STP predeterminada de 32.769 en la VLAN 1, 32.770 en la VLAN 2, 32.771 en la VLAN 3, y así sucesivamente.

Costes de puerto por VLAN

Cada interfaz del switch tiene de forma predeterminada su coste STP por VLAN establecido con los valores de coste revisados del IEEE que se mostraron anteriormente en la Tabla 2.6. En los switches de Cisco, el coste STP está basado en la velocidad actual de las interfaces, así si una interfaz negocia el uso de una velocidad menor, el coste STP predeterminado refleja esta menor velocidad para la Tabla 2.6. Si la interfaz negocia una velocidad diferente, el switch cambia dinámicamente el coste de puerto STP también.

Alternativamente, el coste de puerto de un switch se puede configurar, bien para todas las VLANs o bien para cada una de ellas. Una vez configurado, el switch ignora la velocidad negociada en la interfaz, utilizando en cambio el coste establecido.

Resumen de las opciones de configuración de STP

La Tabla 2.12 resume los valores predeterminados para el BID y los costes de puerto, así como los comandos opcionales de configuración tratados en este capítulo.

Tema clave **Tabla 2.12.** Opciones predeterminadas y de configuración de STP.

Opción	Predeterminado	Comando para cambiar el valor predeterminado
ID de puente	Prioridad: 32.768 + ID VLAN	spanning-tree vlan *id-vlan* root {primary | secondary}
	Sistema: una MAC grabada en el switch	spanning-tree vlan *id-vlan* priority *prioridad*
Coste de la interfaz	En la Tabla 2.6: 100 para 10 Mbps, 19 para 100 Mbps, 4 para 1 Gbps, 2 para 10 Gbps.	spanning-tree vlan *id-vlan* cost *coste*
PortFast	No habilitado	spanning-tree prortfast
BPDU Guard	No habilitado	spanning-tree bpduguard enable

Más adelante, la sección de configuración muestra cómo examinar el funcionamiento de STP en una red sencilla, junto con cómo cambiar estos valores opcionales.

Verificación del comportamiento predeterminado en STP

Los siguientes ejemplos se han tomado de una pequeña red con dos switches, como la de la Figura 2.15. En esta red, utilizando la configuración predeterminada, todas las interfaces excepto una en uno de los switches podrán enviar por los enlaces que conectan los switches. El Ejemplo 2.1 muestra varios comandos show. El texto que sigue al ejemplo explica cómo la salida del comando show identifica los detalles de la topología STP creada en la pequeña red.

El Ejemplo 2.1 comienza con la salida del comando show spanning-tree vlan 3 en SW1. Este comando primero muestra tres grupos principales de mensajes: un grupo de mensajes sobre el switch raíz, seguido de otro grupo sobre el switch local, y finaliza con el rol de la interfaz e información de estado. Comparando los ID raíz e ID de puente sombreados en el primer grupo de mensajes, podrá decir rápidamente si el switch local es la raíz porque el ID de puente y el ID de raíz son iguales. En este ejemplo, el switch local (SW1) no es la raíz.

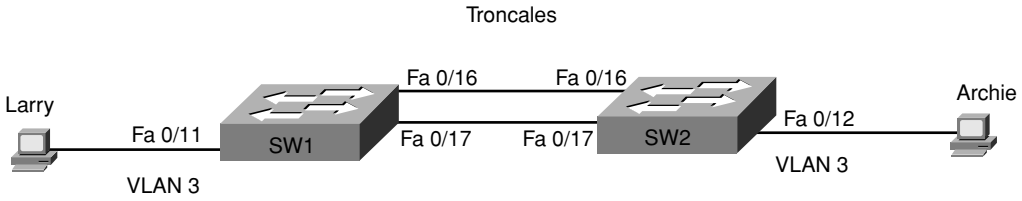


Figura 2.15. Red con dos switches.

Ejemplo 2.1. Estado de STP con parámetros predeterminados.

```
SW1#show spanning-tree vlan 3

VLAN0003
  Spanning tree enabled protocol ieee
  Root ID     Priority    32771
              Address     0019.e859.5380
              Cost        19
              Port        16 (FastEthernet0/16)
              Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID   Priority    32771       (priority 32768 sys-id-ext 3)
              Address     0019.e86a.6f80
              Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time 300

Interface         Role  Sts  Cost    Prio.Nbr   Type
----------------- ---- --- --------- -------- --------------------------------
Fa0/11            Desg  FWD  19      128.11     P2p
Fa0/16            Root  FWD  19      128.16     P2p
Fa0/17            Altn  BLK  19      128.17     P2p
SW1#show spanning-tree root

                                        Root    Hello   Max   Fwd
Vlan                Root ID             Cost    Time    Age   Dly    Root Port
----------------- -------------------- --------- ----- --- --- ------------
VLAN0001        32769 0019.e859.5380   19        2       20    15    Fa0/16
VLAN0002        32770 0019.e859.5380   19        2       20    15    Fa0/16
VLAN0003        32771 0019.e859.5380   19        2       20    15    Fa0/16
VLAN0004        32772 0019.e859.5380   19        2       20    15    Fa0/16
! El siguiente comando proporciona la misma información que el comando show
! spanning-tree vlan 3 acerca del switch local, pero en un formato ligeramente
! breve
SW1#show span vlan 3 bridge

                                                        Hello   Max  Fwd
Vlan                          Bridge ID                 Time   Age   Dly   Protocol
----------------- ---------------------------------------------------------------
VLAN          0003 32771 (32768,   3) 0019.e86a.6f80    2     20    15   ieee!
```

El tercer grupo de mensajes de la salida del comando show spanning-tree vlan 3 identifica parte de la topología STP de este ejemplo, listando todas las interfaces en esa VLAN (tanto las interfaces de acceso como los troncales, que podrían posiblemente soportar la VLAN), sus roles de puerto STP, y sus estados de puerto STP. Por ejemplo, SW1 determina que Fa0/11 juega el rol de un puerto designado porque ninguno de los otros switches ha completado el llegar a ser el DP en ese puerto, como se muestra con el rol de 'desg' en la salida del comando. Por tanto, SW1 debe estar publicando el Hello de menor coste en ese segmento. Como resultado, SW1 ha colocado Fa0/11 en un estado de Envío.

Mientras la salida del comando muestra que SW1 elige la interfaz Fa0/16 como su RP, la lógica aplicada por SW1 para realizar esta elección no aparece en la salida del comando. SW1 recibe BPDUs Hello de SW2 por los puertos Fast Ethernet 0/16 y 0/17, ambos de SW2. Como Fa0/16 y Fa0/17 tienen de forma predeterminada el mismo coste de puerto (19), el coste de SW1 hasta la raíz es el mismo (19) por ambas rutas. Cuando un switch experimenta un empate en el coste para alcanzar la raíz, el switch primero utiliza los valores de **prioridad del puerto** de las interfaces como desempate. Si el valor de prioridad del puerto empata, el switch utiliza el menor número interno de la interfaz. La prioridad de la interfaz y el número de puerto interno aparecen bajo el título "Prio.Nbr" en el Ejemplo 2.1. En este caso, SW1 está utilizando el valor predeterminado de prioridad de puerto de 128 en cada interfaz; así, SW1 utiliza el menor número interno de puerto, Fa0/16, como su puerto raíz, de modo que coloca Fa0/16 en estado Envío.

Obsérvese que la salida del comando muestra Fa0/17 para jugar el rol de un puerto (raíz) alternativo, que se muestra con la abreviatura "Altn". Aunque el rol de puerto alternativo es un concepto de RSTP, la implementación STP 802.1d de Cisco también utiliza este concepto; por tanto, el comando show lista el rol de puerto alternativo. Sin embargo, ya que este puerto no es ni RP ni DP, SW1 coloca este puerto en un estado de Bloqueo.

El siguiente comando del ejemplo, show spanning-tree root, lista el ID de puente del switch raíz en cada VLAN. Observe que ambos switches están utilizando los valores predeterminados, así SW2 llega a ser raíz en las cuatro VLANs existentes. Este comando muestra también la parte de prioridad del ID de puente de forma separada, mostrando valores diferentes de prioridad (32.769, 32.770, 32.771 y 32.772) basándose en la extensión del ID del sistema que ha sido anteriormente explicada en este capítulo. El último comando del ejemplo, show spanning-tree vlan 3 bridge id, muestra información acerca del ID de puente del switch local de VLAN 3.

Configuración de costes de puerto de STP y prioridad del switch

El Ejemplo 2.2 muestra cómo impacta en la topología de STP la configuración del coste de puerto y de la prioridad del switch. Primero, en SW1, el coste de puerto se baja en FastEthernet 0/17, lo que hace que la ruta de SW1 a la raíz por Fa0/17 sea mejor que la ruta que sale por Fa0/16; por tanto, el puerto raíz de SW1 cambia. A continuación de esto, el ejemplo muestra a SW1 como el switch raíz mediante el cambio de la prioridad de puente de SW1.

Ejemplo 2.2. Manipulación del coste de puerto de STP y de la prioridad de puente.

```
SW1#debug spanning-tree events
Spanning Tree event debugging is on
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface Fa0/17
SW1(config-if)#spanning-tree vlan 3 cost 2
00:45:39: STP: VLAN0003 new root port Fa0/17, cost 2
00:45:39: STP: VLAN0003 Fa0/17 -> listening
00:45:39: STP: VLAN0003 sent Topology Change Notice on Fa0/17
00:45:39: STP: VLAN0003 Fa0/16 -> blocking
00:45:54: STP: VLAN0003 Fa0/17 -> learning
00:46:09: STP: VLAN0003 sent Topology Change Notice on Fa0/17
00:46:09: STP: VLAN0003 Fa0/17 -> forwarding
SW1(config-if)#^Z
SW1#show spanning-tree vlan 3

VLAN0003
  Spanning tree enabled protocol ieee
  Root ID     Priority    32771
              Address     0019.e859.5380
              Cost        2
              Port        17 (FastEthernet0/17)
              Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID   Priority    32771 (priority 32768 sys-id-ext 3)
              Address     0019.e86a.6f80
              Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time  15

Interface         Role Sts Cost      Prio.Nbr Type
----------------- ---- --- --------- -------- --------------------------------
Fa0/11            Desg FWD 19        128.11 P2p
Fa0/16            Altn BLK 19        128.16 P2p
Fa0/17            Root FWD 2         128.17 P2p
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#spanning-tree vlan 3 root primary
00:46:58:  setting bridge id (which=1) prio 24579 prio cfg 24576 sysid 3
   (on) id 6003.0019.e86a.6f80
00:46:58: STP: VLAN0003 we are the spanning tree root
00:46:58: STP: VLAN0003 Fa0/16 -> listening
00:46:58: STP: VLAN0003 Topology Change rcvd on Fa0/16
00:47:13: STP: VLAN0003 Fa0/16 -> learning
00:47:28: STP: VLAN0003 Fa0/16 -> forwarding!
```

Este ejemplo empieza con el comando debug spanning-tree events en SW1. Este comando le dice al switch que emita mensajes informativos cuando STP realice cambios en el rol o en el estado de la interfaz. Estos mensajes se presentan en el ejemplo como resultado de la salida de los comandos ejecutados.

Después, se cambia el coste de puerto de la interfaz FastEthernet 0/17 de SW1, sólo en VLAN 3, utilizando el comando spanning-tree vlan 3 cost 2, en el modo de configuración de la interfaz Fa0/17. Inmediatamente después de este comando, SW1 muestra el primer mensaje de depuración significativo. Estos mensajes declaran básicamente que Fa0/17 es ahora el puerto raíz de SW1, que Fa0/16 cambia inmediatamente a un estado de Bloqueo, y que Fa0/17 cambia lentamente a un estado de Envío pasando primero por los estados de Escucha y Aprendizaje. Se pueden ver los 15 segundos (por el valor predeterminado del retardo de envío) en los estados de Aprendizaje y Escucha como se muestra en las marcas de tiempo sombreadas del ejemplo.

Nota

La mayoría de los comandos para establecer los valores de los parámetros STP pueden omitir el parámetro vlan, cambiando así una configuración para todas las VLANs. Por ejemplo, el comando spanning-tree cost 2 podría cambiar el coste STP de una interfaz a 2 para todas las VLANs.

Siguiendo el primer conjunto de mensajes de depuración, la salida del comando show spanning-tree muestra a la interfaz FastEthernet 0/16 como bloqueada y a FastEthernet 0/17 enviando, con el coste al puente raíz ahora de sólo 2, debido al cambio de coste de la interfaz FastEthernet 0/17.

El siguiente cambio ocurre cuando se ejecuta en SW1 el comando spanning-tree vlan 3 root primary. Este comando cambia la prioridad base a 24.576, haciendo que la prioridad de la VLAN 3 de SW1 sea 24.576 más 3, o 24.579. Como resultado, SW1 llega a ser el switch raíz, como se muestra en los mensajes de depuración que siguen.

El comando spanning-tree vlan *id-vlan* root primary le dice al switch que utilice un valor particular de prioridad sólo en esa VLAN, un valor que le permita llegar a ser el switch raíz en esa VLAN. Para hacer esto, este comando establece la prioridad base (el valor de prioridad que se suma al ID VLAN para calcular la prioridad del switch) a un valor menor que la prioridad base del switch raíz actual. Este comando elige la prioridad base como sigue:

- 24.576, si la raíz actual tiene una prioridad mayor de 24.576.
- 4096 menos que el valor actual de prioridad base de la raíz si la prioridad actual de la raíz es 24.576 o menor.

El comando spanning-tree vlan *id-vlan* root secondary le dice al switch que utilice un valor de prioridad base de forma que el switch local se convierta en la raíz si el switch raíz principal falla. Este comando establece el valor de prioridad base del switch a 28.672 independientemente del valor de prioridad de la raíz actual.

Observe que la prioridad también se puede establecer de forma explícita con el comando de configuración global spanning-tree vlan *id-vlan* priority *valor*, que establece la prioridad base del switch. Sin embargo, ya que muchos diseños de LAN cuentan con una raíz desconocida, con un respaldo de la raíz, los otros comandos son típicamente los preferidos.

Configuración de PortFast y BPDU GUARD

Las características PortFast y BPDU Guard pueden configurarse fácilmente en cualquier interfaz. Para configurar PortFast, utilice el subcomando de interfaz spanning-tree portfast. Para habilitar también BPDU Guard, ejecute el subcomando de interfaz spanning-tree bpduguard enable.

Configuración de EtherChannel

Finalmente, los dos switches tienen dos conexiones Ethernet paralelas que pueden ser configuradas como EtherChannel. Al hacer esto, STP no bloquea ninguna interfaz, ya que STP trata ambas interfaces en cada switch como un único enlace. El Ejemplo 2.3 muestra la configuración de SW1 y los comandos show para el nuevo EtherChannel.

Ejemplo 2.3. Configurando y monitorizando EtherChannel.

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface fa 0/16
SW1(config-if)#channel-group 1 mode on
SW1(config)#int fa 0/17
SW1(config-if)#channel-group 1 mode on
SW1(config-if)#^Z
00:32:27: STP: VLAN0001 Po1 -> learning
00:32:42: STP: VLAN0001 Po1 -> forwarding

SW1#show spanning-tree vlan 3

VLAN0003
  Spanning tree enabled protocol ieee
  Root ID    Priority    28675
             Address     0019.e859.5380
             Cost        12
             Port        72 (Port-channel1)
             Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    28675 (priority 28672 sys-id-ext 3)
             Address     0019.e86a.6f80
             Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr    Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/11           Desg FWD 19        128.11      P2p
Po1              Root FWD 12        128.72      P2p
SW1#show etherchannel 1 summary
```

(continúa)

Ejemplo 2.3. Configurando y monitorizando EtherChannel *(continuación).*

```
Flags:  D - down         P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby  (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use:  1
Number of aggregators:            1

Group   Port-channel   Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1       Po1(SU)         -           Fa0/16(P)      Fa0/17(P)!
```

En los switches 2960, cualquier puerto puede ser parte de un EtherChannel, con hasta ocho en un solo EtherChannel; así, los comandos EtherChannel son subcomandos de interfaz. El subcomando de interfaz `channel-group 1 mode on` habilita EtherChannel en las interfaces FastEthernet 0/16 y 0/17. Ambos switches deben estar de acuerdo en el número de EtherChannel, 1 en este caso; por tanto, la configuración *portchannel* de SW2 es idéntica a la de SW1.

El comando `channel-group` permite por configuración de una interfaz que ésta sea siempre un canal de puerto (usando la palabra clave `on`), o bien negociar dinámicamente con otro switch usando las palabras clave `auto` o `desirable`. Utilizando la palabra clave `on` en SW1, si por alguna razón SW2 no estuviera correctamente configurado para EtherChannel, los switches podrían no enviar tráfico por las interfaces.

Alternativamente, el comando de configuración de EtherChannel `channel-group` en cada switch podría usar los parámetros `auto` o `desirable` en lugar de `on`. Con estos otros parámetros, los switches negocian si usar EtherChannel. Si hay acuerdo, se forma un EtherChannel. Si no, los puertos pueden ser utilizados sin formar un EtherChannel, con STP bloqueando algunas interfaces.

El uso de los parámetros `auto` y `desirable` puede ser engañoso. ¡Si se configura `auto` en ambos switches, el EtherChannel nunca se formará! La palabra clave `auto` le dice al switch que espere a que otro switch comience las negociaciones. Tan pronto como uno de los dos switches es configurado como `on` o `desirable`, el EtherChannel puede ser negociado satisfactoriamente.

En el resto del Ejemplo 2.3, se pueden ver varias referencias a "port-channel" o "Po". Ya que STP trata el EtherChannel como un enlace, el switch necesita alguna manera de representar el EtherChannel completo.

El IOS 2960 utiliza el término "Po", abreviatura de "port channel", como una manera de dar nombre al EtherChannel. (EtherChannel también recibe el nombre de canal de puerto). Por ejemplo, cerca del final del ejemplo, el comando `show etherchannel 1 summary` se refiere a Po1, para el canal de puerto/EtherChannel 1.

Configuración de RSTP

La configuración y verificación de RSTP son increíblemente **simples** después de entender completamente las opciones de configuración de STP tratadas en este capítulo. Cada switch necesita un único comando global, spanning-tree mode rapid-pvst. Como puede afirmarse viendo el comando, no sólo se habilita RSTP sino también PVRST, ejecutándose una instancia de RSTP para cada una de las VLANs definidas.

El resto de los comandos de configuración tratados en esta sección se aplican sin cambios a RSTP y PVRST. Los mismos comandos impactan en el BID, el coste de puerto y EtherChannels. De hecho, el subcomando de interfaz spanning-tree portfast todavía funciona, técnicamente haciendo que la interfaz sea una interfaz de tipo contorno, en vez de un tipo enlace, y colocando instantáneamente la interfaz en un estado de Envío.

El Ejemplo 2.4 muestra un ejemplo de cómo migrar desde STP y PVST+ a RSTP y PVRST, y cómo decir si un switch está utilizando RSTP o STP.

Ejemplo 2.4. Configuración y verificación de RSTP y PVRST.

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#spanning-tree mode ?
  mst         Multiple spanning tree mode
  pvst        Per-Vlan spanning tree mode
  rapid-pvst  Per-Vlan rapid spanning tree mode

! La siguiente línea configura este switch para utilizar RSTP y PVRST.
!
SW1(config)#spanning-tree mode rapid-pvst
SW1(config)#^Z
! El texto sombreado "protocol RSTP" significa que este switch utiliza RSTP,
! no STP IEEE.
SW1#show spanning-tree vlan 4

VLAN0004
  Spanning tree enabled protocol rstp
  Root ID    Priority    32772
             Address     0019.e859.5380
             Cost        19
             Port        16 (FastEthernet0/16)
             Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    32772 (priority 32768 sys-id-ext 4)
             Address     0019.e86a.6f80
             Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr  Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/16           Root FWD 19        128.16    P2p Peer(STP)
Fa0/17           Altn BLK 19        128.17    P2p Peer(STP)!
```

Es particularmente importante tomarse el tiempo necesario para comparar la frase sombreada "protocol rstp" del ejemplo con la salida del comando show spanning-tree de los ejemplos anteriores. Todos los ejemplos anteriores utilizan la configuración predeterminada de STP y PVST+, mostrando el texto "protocol ieee", que se refiere al estándar STP IEEE 802.1d original.

Resolución de problemas de STP

La sección final se centra en cómo aplicar la información tratada en las partes anteriores de este capítulo a nuevos escenarios. Aunque esta sección le ayuda a estar preparado para solucionar problemas de STP en redes reales, el objetivo principal de esta sección es prepararle para responder las preguntas de STP en los exámenes CCNA. (Observe que estas secciones no introducen ningún hecho nuevo acerca de STP.)

Las preguntas de STP tienden a intimidar a muchos de los que realizan el test. Una razón de que STP cause problemas a los que realizan el test es que incluso aquellos con experiencia laboral podrían no haber necesitado nunca solucionar problemas de STP. STP se ejecuta de forma predeterminada y funciona bien usando los valores de configuración predeterminados; por tanto, los ingenieros rara vez necesitan solucionar problemas de STP. También, aunque la teoría y los comandos tratados en este capítulo pueden haber sido entendidos, aplicar muchos de estos conceptos y comandos a un único problema en el examen lleva tiempo.

Esta sección describe y resume un plan de ataque para analizar y contestar diferentes tipos de problemas de STP en el examen. Algunas preguntas del examen podrían preguntar qué interfaces deberían enviar o bloquear. Otras preguntas podrían querer conocer qué switch es la raíz, qué puertos son puertos raíz, y qué puertos son puertos designados. Ciertamente, también existen otros tipos de preguntas. Independientemente del tipo de preguntas, los siguientes tres pasos pueden ayudar a analizar STP en cualquier LAN, y, a la vez, contestar cualquier pregunta del examen:

Paso 1 Determine el switch raíz.

Paso 2 Para cada switch no raíz, determine su puerto raíz (RP) y el coste para alcanzar el switch raíz a través de ese RP.

Paso 3 Para cada segmento, determine el puerto designado (DP) y el coste publicado por el DP en ese segmento.

Las siguientes secciones revisan los puntos clave de cada uno de estos pasos, y después presentan algunos trucos para ayudarle a encontrar rápidamente la respuesta a las preguntas del examen.

Determinación del switch raíz

Determinar el switch raíz de STP es fácil si se conocen los BIDs de todos los switches; elija el valor menor. Si la pregunta muestra la prioridad y la dirección MAC separadamen-

te, como es común en la salida de los comandos show, elija el switch con la menor prioridad, o en caso de empate, seleccione el valor menor de dirección MAC.

Si una pregunta requiere la ejecución de comandos show en varios switches para encontrar el switch raíz, una estrategia organizada puede ayudar a responder las preguntas más rápido. Primero, recuerde que distintas variantes del comando show spanning-tree muestran el BID de la raíz, con la prioridad en una línea y la dirección MAC en la siguiente, en la primera parte de la salida; el BID del switch local se lista en la siguiente sección. (En el Ejemplo 2.1 lo tiene sombreado). Recuerde también que los switches de Cisco utilizan de forma predeterminada PVST+; por tanto, tenga cuidado al consultar los detalles de STP para la VLAN correcta. Con estos hechos en mente, la siguiente lista esboza una buena estrategia:

Paso 1 Elija un switch por el que comenzar, y encuentre el BID del switch raíz y el BID del switch local en la VLAN en cuestión con el comando exec show spanning-tree vlan *id-vlan*.

Paso 2 Si el BID raíz y el local son iguales, el switch local es el switch raíz.

Paso 3 Si el BID raíz no es igual al BID del switch local, siga estos pasos:

- **a.** Localice la interfaz RP en el switch local (también en la salida del comando show spanning-tree).
- **b.** Utilizando el Protocolo de descubrimiento de Cisco (CDP, *Cisco Discovery Protocol*) u otra documentación, determine qué switch está en el otro extremo de la interfaz RP encontrada en el Paso 3A.
- **c.** Entre en el switch del otro extremo de la interfaz RP y repita este proceso, comenzando en el Paso 1.

El Ejemplo 2.5 muestra la salida de un comando show spanning-tree vlan 1. Sin ni siquiera conocer la topología de la LAN, tómese tiempo ahora para probar esta estrategia de resolución de problemas basándose en la salida del ejemplo, y compare sus pensamientos con las explicaciones que siguen a este ejemplo.

Ejemplo 2.5. Localización del switch raíz.

```
SW2#show spanning-tree vlan 1
VLAN0001
Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000a.b7dc.b780
              Cost        19
              Port        1 (FastEthernet0/1)
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID   Priority    32769 (priority 32768 sys-id-ext 1)
              Address     0011.92b0.f500
              Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time 300
```

(continúa)

Ejemplo 2.5. Localización del switch raíz *(continuación).*

```
Interface         Role Sts Cost      Prio.Nbr  Type

----------------- ---- --- --------- -------- --------------------------------
Fa0/1             Root FWD 19        128.1     P2p
Fa0/19            Desg FWD 100       128.19    Shr
Fa0/20            Desg FWD 100       128.20    Shr
SW2#show spanning-tree vlan 1 bridge id
VLAN0001 8001.0011.92b0.f500
```

La porción sombreada del ejemplo señala el BID de la raíz (prioridad y dirección) así como el BID diferente de SW2. Ya que el BID del switch raíz es diferente, el siguiente paso debería ser encontrar el puerto raíz, que aparece en dos lugares diferentes en la salida del comando (Fa0/1). El siguiente paso podría ser repetir el proceso en el switch del otro extremo de la interfaz Fa0/1 de SW2, pero el ejemplo no identifica a este switch.

Determinación del puerto raíz en los switches que no son raíz

Cada switch no raíz tiene un, y sólo un, puerto raíz (RP). (Los switches raíz no tienen un RP.) Para elegir su RP, un switch escucha las BPDUs Hello entrantes. Para cada Hello recibido, el switch añade el coste escuchado en la BPDU Hello al coste de puerto de ese switch para el puerto por el que se recibió el Hello. El menor coste calculado gana; en caso de empate, el switch elige la interfaz con la menor prioridad de puerto, y en caso de empate, el switch elige el menor número interno de puerto.

Mientras el párrafo anterior resume cómo un switch no raíz elige su RP, cuando una pregunta del examen proporciona información acerca del switch raíz y los costes de interfaz, es posible que un planteamiento ligeramente diferente pueda acelerar su camino hacia la respuesta. Por ejemplo, considere la siguiente pregunta, acerca de la red mostrada en la Figura 2.16:

> En la red con switches mostrada en la Figura 2.16, todos los switches y segmentos están funcionando, con STP habilitado en la VLAN 1. SW1 ha elegido la raíz. La interfaz Fa0/1 de SW2 utiliza un coste establecido a 20; todas las demás interfaces utilizan el coste predeterminado de STP. Determine el RP en SW4.

Una manera de solucionar este problema consiste en aplicar los conceptos de STP resumidos en el primer párrafo de esta sección. Alternativamente, se puede encontrar la solución un poco más rápidamente con el siguiente proceso, comenzando por un switch no raíz:

Paso 1 Determine todas las posibles rutas por las cuales una trama, enviada por el switch no raíz, puede alcanzar el switch raíz.

Paso 2 Para cada posible ruta del Paso 1, añada el coste de todas las interfaces de salida en esa ruta.

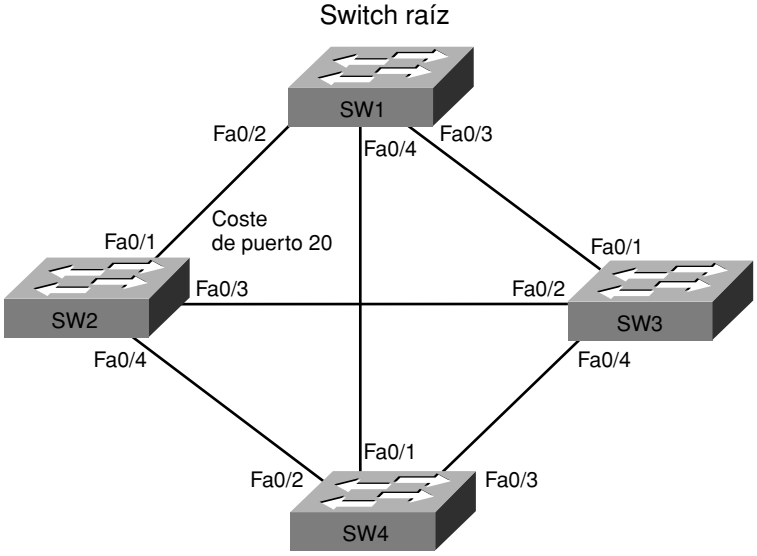


Figura 2.16. Análisis de STP: ejemplo 1.

Paso 3 El menor coste encontrado es el coste para alcanzar la raíz, y la interfaz de salida es el RP del switch.

Paso 4 Si el coste empata, utilice la prioridad del puerto como desempate, y si persiste el empate, utilice el menor número interno para desempatar.

La Tabla 2.13 muestra el trabajo realizado en los Pasos 1 y 2 de este proceso, mostrando las rutas y los costes respectivos para alcanzar la raíz por cada ruta. En esta red, SW4 tiene cinco posibles rutas hacia el switch raíz. La columna Coste lista los costes en el mismo orden que en la primera columna, junto con el coste total.

Tabla 2.13. Localización del RP de SW4: calculando el coste.

Ruta física (interfaces salientes)	Coste
SW4 (Fa0/2) –> SW2 (Fa0/1) –> SW1	19 + 20 = 39
SW4 (Fa0/3) –> SW3 (Fa0/1) –> SW1	19 + 19 = 38
SW4 (Fa0/1) –> SW1	19 = 19
SW4 (Fa0/2) –> SW2 (Fa0/3) –> SW3 (Fa0/1) –> SW1	19 + 19 + 19 = 57
SW4 (Fa0/3) –> SW3 (Fa0/2) –> SW2 (Fa0/1) –> SW1	19 + 19+ 20 = 58

Simplemente para asegurar que los contenidos de la tabla están claros, examine por un momento la ruta física SW4 (Fa0/2) –> SW2 (Fa0/1) –> SW1. Para esta ruta, las interfaces salientes son la interfaz Fa0/2 de SW4, coste predeterminado 19, y la interfaz Fa0/1 de SW2, configurada con un coste de 20, para un total de 39.

Se debería también comprobar qué costes de interfaces se ignoran con este proceso. Usando el mismo ejemplo, la trama enviada por SW4 hacía la raíz podría entrar por la interfaz Fa0/4 de SW2 y la interfaz Fa0/2 de SW1. Ningún otro coste de las interfaces podría ser considerado.

En este caso, el RP de SW4 podría ser su interfaz FA0/1, ya que la ruta de coste menor (coste 19) comienza por esta interfaz.

Tenga cuidado en dar por ciertas algunas cosas en las preguntas en las que necesite encontrar el RP de un switch. Por ejemplo, en este caso, podría pensar intuitivamente que el RP de SW4 podría ser su interfaz Fa0/1, ya que está directamente conectada a la raíz. Sin embargo, si en las interfaces Fa0/3 de SW4 y Fa0/1 de SW3 se ha configurado un coste de puerto de 4 en cada una, la ruta SW4 (Fa0/3) –> SW3 (Fa0/1) – > SW1 tendría un coste total de 8, y el RP de SW4 sería su interfaz Fa0/3. Por tanto, sólo porque la ruta parece mayor en el diagrama, recuerde que el punto de decisión es el coste total.

Determinando el puerto designado en cada segmento de LAN

Cada segmento de LAN tiene un único switch que actúa como el puerto designado (DP) en ese segmento. En segmentos que conectan un switch con un dispositivo que no utiliza STP (por ejemplo, segmentos que conectan un switch con un PC o un router), el puerto del switch es elegido como el DP porque el único dispositivo enviando un Hello en el segmento es el switch. Sin embargo, los segmentos que conectan múltiples switches necesitan un poco más de trabajo para determinar quien debe ser el DP. Por definición, el DP para un segmento se determina como sigue:

> La interfaz del switch que envía la BPDU Hello de menor coste en el segmento es el DP. En caso de empate, entre los switches que están enviando los Hellos cuyos costes empatan, el switch con el menor BID gana.

De nuevo, la definición formal describe qué hace STP, y este concepto se puede aplicar en cualquier pregunta de STP. Sin embargo, para los exámenes, si encuentra el RP de cada switch no raíz, y anota el coste para alcanzar la raíz en cada switch (por ejemplo, como se muestra en la Tabla 2.13), puede encontrar fácilmente el DP como sigue:

Paso 1 Para los switches conectados al mismo segmento de LAN, el switch con el coste menor para alcanzar la raíz es el DP en ese segmento.

Paso 2 En caso de empate, entre los switches que empatan en coste, el switch con el menor BID llega a ser el DP.

Por ejemplo, considere la Figura 2.17. Esta figura muestra la misma red conmutada de la Figura 2.16, pero indicando los RPs y DPs, así como el coste menor para alcanzar la raíz del switch a través de sus respectivos RP.

Centrémonos por el momento en los segmentos que conectan los switches no raíces. Para el segmento SW2–SW4, SW4 gana por virtud de tener un coste de 19 en su ruta hasta la raíz, considerando que la mejor ruta de SW2 es de coste 20. Por la misma razón, SW3 lle-

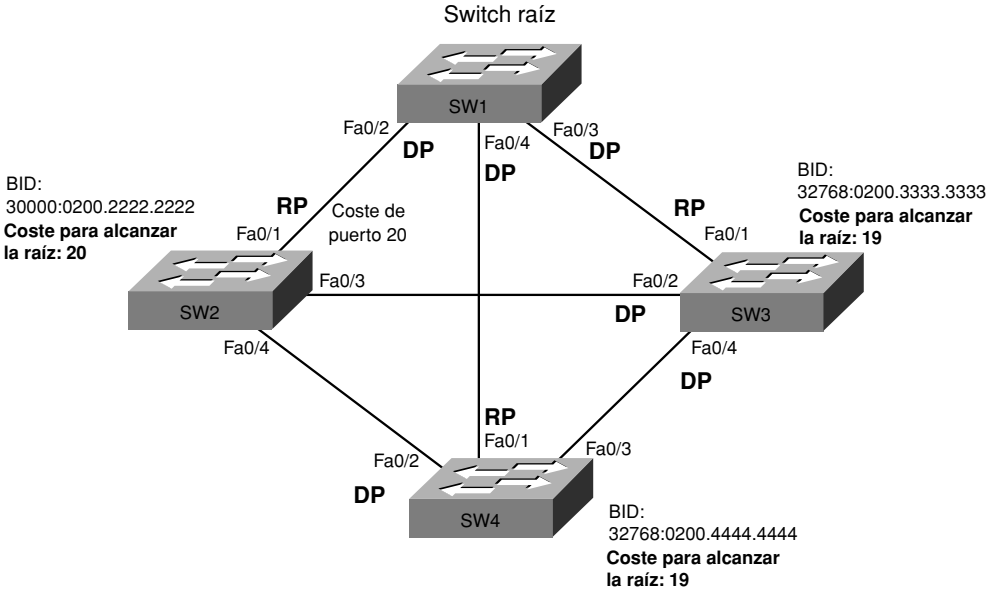


Figura 2.17. Elección de los puertos designados.

ga a ser el DP en el segmento SW2–SW3. Para el segmento SW3–SW4, tanto SW3 como SW4 empatan en coste para alcanzar la raíz. La figura muestra los BIDs de los switches no raíces; por tanto, se puede ver que el BID de SW3 es menor. Como resultado, SW3 gana el desempate, por lo que se convierte en el DP en ese segmento.

Observe también que el switch raíz (SW1) llega a ser el DP en todos sus segmentos en virtud del hecho de que el switch raíz siempre publica Hellos de coste 0, y el coste calculado de todos los demás switches debe ser al menos 1, ya que el coste de puerto mínimo permitido es 1.

Para los exámenes, debe ser capaz de encontrar el switch raíz, después el RP en cada switch, y después el DP en cada segmento; después conocerá los BIDs, los costes de puerto y la topología de la LAN. En este punto, también conoce qué interfaces envían (aquellas interfaces que son RPs o DPs), con el resto de interfaces bloqueadas.

Convergencia de STP

La topología de STP (el conjunto de interfaces en un estado de Envío) debe permanecer estable mientras la red permanezca estable. Cuando los interfaces y los switches comiencen a funcionar o dejen de hacerlo, la topología resultante puede cambiar; dicho de otra forma, se producirá la convergencia de STP. Esta sección señala una pequeña estrategia de sentido común para afrontar este tipo de problemas en los exámenes.

Algunas preguntas del examen relativas a STP podrían ignorar los detalles de la transición cuando ocurre la convergencia; en cambio, se pueden centrar en qué interfaces cam-

bian de Envío a Bloqueo, o de Bloqueo a Envío, cuando se produce un cambio concreto. Por ejemplo, una pregunta podría especificar los detalles de un escenario y después preguntar, "¿Qué interfaces cambiarían de un estado de Bloqueo a Envío?" Para estas preguntas que comparan las topologías anterior y posterior a un cambio, aplique los mismos pasos ya tratados en esta sección, pero dos veces: una para las condiciones anteriores al cambio y otra para las condiciones que causan el cambio.

Otras preguntas de STP podrían centrarse en el proceso de transición, incluyendo el temporizador Hello, el temporizador de Edad máxima, el temporizador de retardo de envío, los estados de Escucha y Aprendizaje, y sus usos, como ya se han descrito en este capítulo. Para este tipo de preguntas, recuerde los siguientes hechos sobre lo que ocurre durante la convergencia de STP:

- Para las interfaces que están en el mismo estado de STP, nada necesita cambiar.
- Para las interfaces que necesitan cambiar de un estado de Envío a un estado de Bloqueo, el switch cambia inmediatamente su estado a Bloqueo.
- Para las interfaces que necesitan cambiar de un estado de Bloqueo a un estado de Envío, el switch primero mueve la interfaz al estado de Escucha, y después al estado de Aprendizaje, cada uno durante el tiempo especificado en el temporizador de retardo de envío (15 segundos de forma predeterminada). Sólo entonces la interfaz pasa al estado de Envío.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 2.14 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 2.14. Temas clave del Capítulo 2.

Tema Clave	Descripción	Número de página
Tabla 2.2	Lista los tres principales problemas que ocurren cuando no se utiliza STP en una LAN con enlaces redundantes.	62
Tabla 2.3	Lista las razones por las que un switch elige colocar una interfaz en un estado de Envío o de Bloqueo.	65
Tabla 2.4	Muestra los campos más importantes de los mensajes BPDU Hello.	66
Figura 2.5	Muestra cómo los switches calculan sus costes raíz.	69
Tabla 2.6	Lista los costes de puerto STP original y actual predeterminados para distintas velocidades de interfaz.	70
Lista	Una descripción resumida de los estados estables de operación de STP.	71
Tabla 2.7	Temporizadores de STP.	71
Lista	Definiciones de qué ocurre en los estados de Escucha y Aprendizaje.	73
Tabla 2.8	Resumen de los estados 802.1d.	73
Lista	Similitudes entre RSTP y STP.	76
Tabla 2.9	Lista los estados de interfaz de 802.1d y los correspondientes de 802.1w.	78
Tabla 2.10	Lista los roles de puerto de STP y RSTP y los compara.	80

(continúa)

Tabla 2.14. Temas clave del Capítulo 2 *(continuación).*

Tema Clave	Descripción	Número de página
Figura 2.13	Vista conceptual de los beneficios del equilibrado de la carga de PVST+.	85
Tabla 2.11	Compara tres opciones para múltiples árboles de extensión.	86
Figura 2.14	Muestra el formato de la extensión del ID del sistema del campo de prioridad de STP.	87
Tabla 2.12	Lista los valores predeterminados de algunos parámetros de configuración opcionales de STP y los comandos de configuración relacionados.	88
Lista	Dos ramas de la lógica de cómo el comando spanning-tree root primary elige una nueva prioridad base de STP.	92
Lista	Estrategia para resolver problemas de STP en los exámenes.	96

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD) o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe sus respuestas en el glosario.

BPDU Guard, BPDU Hello, Edad máxima, estado de Aprendizaje, estado de Descarte, estado de Envío, estado de Escucha, EtherChannel, Hello inferior, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, ID de puente, PortFast, Protocolo de árbol de extensión (STP), Protocolo de árbol de extensión rápido (RSTP), Puerto alternativo, puerto deshabilitado, Puerto de respaldo, puerto designado, puerto raíz, retardo de envío, switch raíz, Unidad de datos del protocolo de puentes (BPDU).

Referencias de comandos

Aunque no necesariamente debe memorizar la información de las tablas de esta sección, ésta incluye una referencia de los comandos de configuración y EXEC utilizados en este capítulo. En la práctica, debería memorizar los comandos como un efecto colateral de leer el capítulo y hacer todas las actividades de esta sección de preparación del examen. Para verificar si ha memorizado los comandos como un efecto colateral de sus otros estudios, cubra el lado izquierdo de la tabla con un trozo de papel, lea las descripciones del lado derecho, y compruebe si recuerda el comando.

Tabla 2.15. Referencia de Comandos de configuración del Capítulo 2.

Comando	Descripción
spanning-tree vlan *número-vlan* root primary	Comando de configuración global que cambia este switch a switch raíz. La prioridad del switch cambia al menor de 24.576 ó 4096 menos que la prioridad del actual puente raíz cuando se ejecuta el comando.
spanning-tree vlan *número-vlan* root secondary	Comando de configuración global que establece la prioridad base STP del switch a 28.672.
Spanning-tree [vlan *id-vlan*] {priority *prioridad*}	Comando de configuración global que cambia la prioridad de puente de este switch para la VLAN especificada.
Spanning-tree [vlan *número-vlan*] cost *coste*	Subcomando de interfaz que cambia el coste STP al valor configurado.
channel-group *número-grupo-canal* mode {auto | desirable | on}	Comando de configuración global que cambia la prioridad de puente de este switch para la VLAN especificada.
spanning-tree portfast	Subcomando de interfaz que habilita PortFast en la interfaz.
spanning-tree bpduguard enable	Subcomando de interfaz para habilitar BPD Guard en una interfaz.
spanning-tree mode {mst | rapid-pvst|pvst}	Comando global para habilitar PVST+ y 802.1d (pvst), PVRST y 802.1w (rapid-pvst), o IEEE 802.1s (múltiples árboles de extensión) y v 802.Iw (mst).

Tabla 2.16. Comandos EXEC del Capítulo 2.

Comando	Descripción
show spanning-tree	Muestra los detalles acerca del estado de STP en el switch, incluyendo el estado de cada puerto.

(continúa)

Tabla 2.16. Comandos EXEC del Capítulo 2 *(continuación)*.

Comando	Descripción
show spanning-tree interface *interfaz*	Muestra información de STP sólo para el puerto especificado.
show spanning-tree vlan *id-vlan*	Muestra información de STP para la VLAN especificada.
show spanning-tree [vlan *id-vlan*] root	Muestra información acerca de la raíz de cada VLAN o sólo de la VLAN especificada.
show spanning-tree [vlan *id-vlan*] bridge	Lista información de STP acerca del switch local para cada VLAN o sólo para la VLAN especificada.
debug spanning-tree evenst	Provoca que el switch proporcione mensajes de información acerca de los cambios en la topologtía de STP.
show etherchannel [*número-grupo-canal*] {brief | detail | port | port-channel | summary}	Muestra información acerca del estado de EtherChannel en este switch.

Este capítulo trata los siguientes temas:

Metodologías generales de resolución de problemas: Esta sección presenta discusiones y opiniones acerca de cómo plantear un problema de red cuando una explicación general del problema no identifica rápidamente la causa raíz.

Resolución de problemas en el plano de datos de conmutación LAN: Esta sección sugiere varios pasos organizados para solucionar problemas en una LAN Ethernet, con una revisión detallada de comandos y métodos.

Predicción del funcionamiento normal del plano de datos de conmutación LAN: Esa sección sugiere cómo analizar la salida de los comandos `show` en un switch y las figuras para predecir por dónde será enviada una trama en una red LAN conmutada de ejemplo.

CAPÍTULO 3

Resolución de problemas de conmutación LAN

Este capítulo, junto con los Capítulos 7 y 11, realizan un importante trabajo: ayudarle a desarrollar las habilidades de resolución de problemas necesarias para contestar de forma rápida y confiada ciertos tipos de preguntas en los exámenes. Al mismo tiempo, este capítulo espera prepararle mejor para solucionar problemas en las redes reales.

NOTA

Para algunas reflexiones de por qué la resolución de problemas es tan importante para los exámenes, refiérase a la sección "Formato de los exámenes CCNA" en la introducción de este libro.

Los capítulos de resolución de problemas de este libro no tienen el mismo objetivo principal que los otros. Expuesto de forma sencilla, los capítulos que no tratan la resolución de problemas se centran en características y hechos individuales acerca de un área de la tecnología, mientras que los capítulos de resolución de problemas reúnen un conjunto más amplio de conceptos mezclados. Estos capítulos de resolución de problemas tienen una visión más amplia del mundo de las redes, centrándose en cómo las partes trabajan juntas, asumiendo que ya se conocen los componentes individuales.

Este capítulo trata la misma tecnología tratada en los otros capítulos de esta parte del libro (Capítulos 1 y 2,) y los materiales prerrequisitos relacionados (como los tratados en *Guía Oficial para el examen de Certificación CCENT/CCNA ICND1*). Además, ya que este capítulo es el primer capítulo de resolución de problemas en este libro, también explica algunos conceptos generales acerca de la metodología de resolución de problemas.

Cuestionario "Ponga a prueba sus conocimientos"

Ya que los capítulos de resolución de problemas de este libro reúnen conceptos de varios de los otros capítulos, incluyendo algunos capítulos del libro *CCENT/CCNA ICND1*, y muestran cómo plantear algunas de las preguntas más desafiantes de los exámenes CCNA, debe leer este capítulo con independencia de su actual nivel de conocimientos. Por

esta razón, los capítulos de resolución de problemas no incluyen el cuestionario "Ponga a prueba sus conocimientos". Sin embargo, si se siente particularmente confiado en las características de la resolución de problemas de conmutación LAN tratadas en este libro y en el libro *CCENT/CCNA ICND1*, puede pasar directamente a la sección "Ejercicios para la preparación del examen", cerca del final de este capítulo.

Temas fundamentales

Este capítulo tiene tres secciones principales. La primera sección se centra en el proceso de resolución de problemas como un fin en sí mismo. La segunda sección explica como aplicar los métodos generales de resolución de problemas especialmente desde el plano de datos de conmutación LAN. La última sección presenta entonces algunas sugerencias e ideas acerca de tipos específicos de problemas relativos a la conmutación LAN.

Metodologías generales de resolución de problemas

Nota

Las estrategias y métodos genéricos de resolución de problemas aquí descritos son un medio para un fin. No necesita estudiar estos procesos ni memorizarlos para los propósitos del examen. En cambio, estos procesos pueden ayudarle a razonar los problemas en el examen, por lo que podrá responder las preguntas un poco más deprisa y con un poco más de confianza.

Cuando se presenta la necesidad de resolver un problema de red, todo el mundo utiliza alguna metodología de resolución de problemas, bien informal o formal. Algunas personas comienzan por validar el cableado físico y el estado de las interfaces de todos los enlaces que podrían estar afectados por el problema. Otras prefieren empezar por verificar la accesibilidad de todo lo que pueda decirnos algo más acerca del problema, y después entrar más profundamente en los detalles. Incluso otras, podrían intentar aquello que primero les venga a la cabeza hasta que intuitivamente averigüen el problema general. Ninguno de estos métodos es inherentemente bueno o malo; yo he probado todos estos métodos, e incluso otros, y he tenido algunos aciertos con cada planteamiento.

Mientras que la mayoría de las personas desarrollan hábitos y estilos de resolución de problemas que funcionan bien basados en sus propias experiencias y esfuerzos, una metodología de resolución de problemas más sistemática puede ayudar a cualquiera a apren-

der a solucionar problemas con más éxito. Las siguientes secciones describen una de tales metodologías sistemáticas de resolución de problemas con el propósito de ayudarle a prepararse para solucionar los problemas de red en los exámenes CCNA. Esta metodología de resolución de problemas tiene tres ramas principales, que generalmente tienen lugar en el orden aquí mostrado:

- **Análisis/predicción del funcionamiento normal**. La descripción y predicción detalladas de qué debería pasar si la red está funcionando correctamente, basándose en la documentación, la configuración y la salida de los comandos show y debug.
- **Aislamiento del problema**. Cuando pueda estar ocurriendo algún problema, encontrar el(los) componente(s) que no funciona(n) correctamente comparándolo con el comportamiento previsto, de nuevo basándose en la documentación, configuración y salida de comandos show y debug.
- **Análisis de la causa raíz**. Identificar las causas que subyacen tras los problemas identificados en el paso previo, específicamente las causas que tienen una acción específica con la cuál el problema puede arreglarse.

Siguiendo estos tres pasos el ingeniero debería conocer no solamente los síntomas del problema sino cómo solucionarlo. A continuación, el texto explica algunas reflexiones acerca de cómo plantear cada paso del proceso de resolución de problemas.

Análisis y predicción del funcionamiento normal de la red

El trabajo de cualquier red es entregar datos desde un dispositivo de usuario final a otro. Para analizar la red, un ingeniero necesita entender la lógica que emplea cada dispositivo para enviar datos al siguiente. Razonando sobre lo que debe pasar en cada dispositivo, el ingeniero puede describir el flujo completo de los datos.

El término **plano de datos** se refiere a cualquier acción tomada por los dispositivos de red para el envío de una trama o paquete individual. Para enviar cada trama o paquete, un dispositivo aplica su lógica del plano de datos y procesa la trama o paquete. Por ejemplo, cuando un switch LAN recibe una trama por una interfaz en la VLAN 3, el switch podría tomar la decisión de envío basándose en las entradas de la tabla de direcciones MAC, y enviar el paquete. Toda esta lógica es parte de un procesamiento en el plano de datos del switch.

El término **plano de control** se refiere a la sobrecarga de procesos que no es necesario que se realice para cada paquete o trama. En cambio, algunos procesos del plano de control dan soporte al proceso de envío. Por ejemplo, el Protocolo de *trunking* VLAN (VTP), y los protocolos de enrutamiento IP son ejemplos de procesos del plano de control. Otros procesos del plano de control pueden estar sólo indirectamente relacionados con el plano de datos. Por ejemplo, el Protocolo de descubrimiento de Cisco (CDP) puede ser útil para confirmar si la documentación de la red es correcta, pero CDP puede ser deshabilitado sin efectos en el proceso de envío del plano de datos.

Para predecir el funcionamiento esperado de una red, o explicar los detalles de cómo una red funcionando correctamente está actualmente trabajando, puede ser útil comenzar examinando tanto el plano de control como el plano de datos. Este texto muestra primero el plano de datos, pero en la vida real, se puede comenzar por uno o por otro en función de los síntomas conocidos del problema.

Análisis del plano de datos

La resolución de problemas en el plano de datos examina, en orden, cada dispositivo en la ruta de envío esperada de los datos. El análisis comienza con el host creando el dato original. Este host envía el dato a algún dispositivo, que entonces envía el dato a otro dispositivo, y así sucesivamente, hasta que el dato alcanza el host final. El host destinatario típicamente envía alguna clase de contestación, así que para entender completamente cómo funcionan las comunicaciones útiles, es necesario analizar también el proceso inverso. Concretamente, los síntomas exteriores del problema identifican normalmente los dispositivos de usuario final que no pueden comunicarse, pero el problema subyacente podría estar relacionado sólo con tramas o paquetes viajando en una dirección.

A menos que los síntomas de un problema particular ya sugieran un problema específico, la resolución de problemas en el plano de datos debe empezar con un análisis del plano de datos de la capa 3. Si se empieza con la capa 3, se deben ver los pasos principales en el envío y recepción de datos entre dos hosts. Después se debe examinar cada uno de los pasos de envío de la capa 3 más de cerca, mirando en los detalles subyacentes de los niveles 1 y 2. Por ejemplo, la Figura 3.1 muestra los seis pasos principales del envío IP (plano de datos) en una pequeña red.

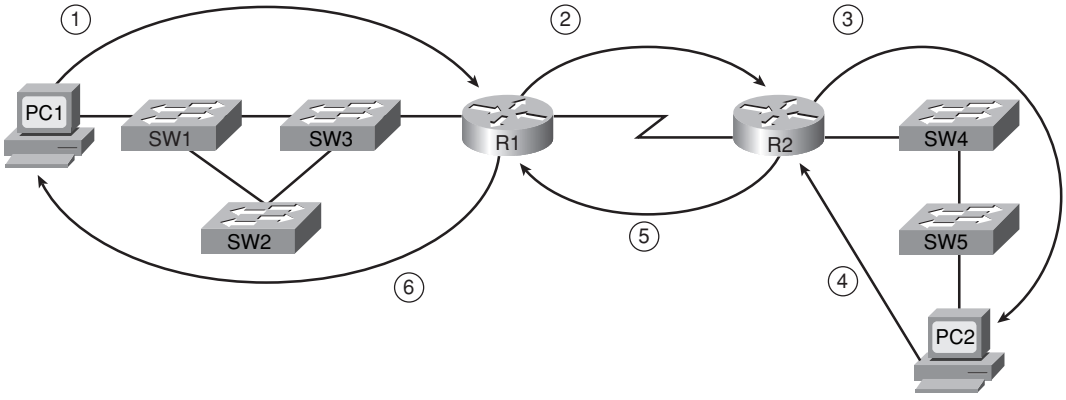


Figura 3.1. Ejemplo de los pasos principales en un envío IP.

Mientras razona el comportamiento esperado de la capa 3 en este caso, podría necesitar considerar cómo el paquete fluye de la izquierda a la derecha, y después cómo la res-

puesta fluye de derecha a izquierda. Usando los seis pasos de la figura, podría hacerse el siguiente análisis:

Paso 1 Pensar en las direcciones y máscaras IP de PC1 y PC2, y en la lógica de PC1 para comprender que PC2 está en otra subred. Esto causa que PC1 elija enviar el paquete a su router predeterminado (R1).

Paso 2 Considerar la lógica de envío de R1 para buscar la dirección IP de destino del paquete en la tabla de enrutamiento de R1, esperando que R1 elija enviar a continuación el paquete al router R2.

Paso 3 En R2, considerar la misma lógica de búsqueda en la tabla de enrutamiento que se utilizó en el paso previo, ahora con la tabla de enrutamiento de R2. La entrada que coincida debería ser una ruta conectada a R2.

Paso 4 Este paso está relacionado con el paquete de respuesta de PC2, que utiliza la misma lógica que el Paso 1. Comparar dirección/máscara IP de PC2 con la dirección/máscara IP de PC1, observando que están en diferentes subredes. Como resultado, PC2 debería enviar el paquete a su router predeterminado, R2.

Paso 5 Considerar la lógica de envío de R2 para paquetes destinados a la dirección IP de PC1, con la expectación de que la ruta elegida debería provocar que R2 enviaron estos paquetes a R1.

Paso 6 El paso de enrutamiento final, en R1, podría mostrar un paquete destinado a la dirección IP de PC1 que coincide con una ruta conectada a R1, que hace que R1 envíe el paquete directamente a la dirección MAC de PC1.

Después de afianzar sus conocimientos del comportamiento esperado de cada paso en la capa 3, debería examinar entonces la capa 2. Siguiendo el mismo orden de nuevo, debería echar un vistazo más detallado al primer paso de enrutamiento de capa 3 de la Figura 3.1 (PC1 enviando un paquete a R1), examinando los detalles de las capas 1 y 2 de cómo la trama la envía PC1 para ser entregada a R1, como se muestra en la Figura 3.2.

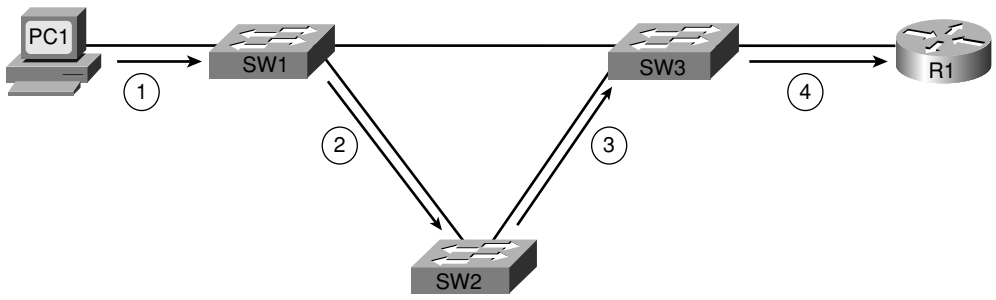


Figura 3.2. Ejemplo de los principales pasos del envío en la conmutación LAN.

Para este análisis, se podría empezar de nuevo con PC1, esta vez considerando la cabecera y la información final de Ethernet, concretamente las direcciones MAC de origen y destino. Entonces, en el Paso 2, se podría considerar la lógica de envío de SW1, que com-

para la dirección MAC de destino de la trama con la tabla de direcciones MAC de SW1, indicando a SW1 que envíe la trama a SW2. Los Pasos 3 y 4 podrían repetir la lógica del Paso 2 desde SW2 a SW3, respectivamente.

Análisis del plano de control

Muchos procesos del plano de control afectan directamente al proceso del plano de datos. Por ejemplo, el enrutamiento IP no puede funcionar sin las apropiadas rutas IP; por ello, los routers utilizan típicamente protocolos dinámicos de enrutamiento (un protocolo del plano de control) para aprender rutas. Los protocolos de enrutamiento se considera que son protocolos del plano de control en parte porque el trabajo realizado por un protocolo de enrutamiento no tiene que repetirse para cada trama o paquete.

Mientras los procesos del plano de datos se prestan por ellos mismos a procesos de resolución de problemas algo genéricos consistentes en examinar la lógica de envío de cada dispositivo, los procesos del plano de control difieren demasiado como para permitir tales procesos generales de resolución de problemas. Sin embargo, es útil considerar un conjunto de pasos específicos de resolución de problemas para cada protocolo específico del plano de control. Por ejemplo, el Capítulo 1 explica cómo plantear la resolución de problemas de varios tipos de problemas de VTP.

Predicción del funcionamiento normal: resumen del proceso

En los exámenes, algunas preguntas podrían simplemente pedirle que analice y prediga el funcionamiento normal de una red operativa. En otros casos, la predicción del comportamiento normal es justo el precursor para aislar y resolver el problema. Con independencia de si la pregunta da o no pistas acerca de en qué parte de la red centrarse, la siguiente lista resume el planteamiento sugerido para encontrar las respuestas:

Paso 1 Examine el plano de datos como sigue:

- **a.** Determine los pasos principales de la capa 3 (incluyendo desde el host de origen hasta el router predeterminado, cada router al siguiente router, y el último router hasta el host de destino) en ambas direcciones.
- **b.** Para cada red de capa 2 entre un host y un router o entre dos routers, analice la lógica de envío en cada dispositivo.

Paso 2 Examine el plano de control como sigue:

- **a.** Identifique los protocolos del plano de control que están usándose y son vitales en el proceso de envío.
- **b.** Examine el funcionamiento apropiado de cada protocolo vital del plano de control; los detalles de este análisis variarán para cada protocolo.
- **c.** Posponga cualquier análisis de los protocolos del plano de control que no afecten a la correcta operación del plano de datos hasta que no vea clara-

mente la necesidad para el protocolo de responder esta pregunta (por ejemplo, CDP).

Aislamiento del problema

El proceso de resolución de problemas rara vez es un proceso secuencial. Para respetar cierta organización, este capítulo presenta el aislamiento del problema como el segundo de tres pasos de la resolución de problemas. Sin embargo, este paso es más probable que ocurra tan pronto como el primer paso (prediciendo el comportamiento normal) encuentre un problema. Así, mientras las listas genéricas mostradas en esta sección ayudan a proporcionar una estructura acerca de cómo solucionar un problema, en la práctica real pueden estar desordenadas.

Cuando no tenga pistas de cómo proceder, otra que no sea que dos hosts no pueden comunicarse, lo mejor es empezar de nuevo con el plano de datos de la capa 3 (con otras palabras, la lógica de envío de IP). Después, cuando se encuentre un paso de envío de IP que no funciona, examine qué paso está más cerca para aislar más allá de donde el problema está ocurriendo. Por ejemplo, considere la Figura 3.1 de nuevo, que muestra un paquete entregado por PC1 a PC2, y vuelta, en seis pasos de enrutamiento. En este caso, sin embargo, se determina que R2 toma el paquete, pero el paquete nunca se entrega a PC2. Por tanto, se debe mirar más de cerca cualquier cosa entre R2 y PC2 para aislar el problema.

Después de aislar el problema a un paso de envío de IP (como se muestra en la Figura 3.1), se debe continuar para aislar el problema con el menor número de componentes como sea posible. Por ejemplo, si R2 toma el paquete, pero PC2 no, el problema podría estar en R2, SW4, SW5, PC2, el cableado, o posiblemente en dispositivos omitidos en la documentación de la red.

El proceso para aislar el problema típicamente requiere razonar acerca de las funciones de varias capas del modelo OSI, así como en las funciones del plano de datos y del plano de control. Continuando con el mismo escenario del problema de ejemplo, para poder enviar paquetes a PC2, R2 necesita conocer la dirección MAC de PC2 aprendida utilizando el Protocolo de resolución de direcciones (ARP, *Address Resolution Protocol*). Si descubre que R2 no tiene una entrada ARP para PC2, debería tender a pensar que existe un cierto tipo de problema relacionado con IP. Sin embargo, este problema podría estar provocado porque el troncal SW4–SW5 no funcione, lo que significa que la petición ARP IP de R2 (una difusión LAN) puede no ser entregada por SW4 a SW5, y después a PC2. Por tanto, el problema con el proceso de envío del paquete de R2 a PC2 podría estar relacionado con un protocolo de control (ARP), pero el fallo de la petición ARP podría estar causado todavía por otros dispositivos (caída del troncal SW4–SW5), que podría ser un problema de las capas 2 ó 1.

Si una pregunta del examen no da pistas de por dónde empezar, el siguiente proceso resume una buena estrategia general y sistemática de aislamiento del problema:

Paso 1 Comenzar examinando el plano de datos de la capa 3 (envío IP), comparando el resultado con el comportamiento normal esperado, hasta identificar el primer paso principal de enrutamiento que falla.

Paso 2 Aislar el problema a la menor cantidad posible de componentes:

a. Examinar las funciones de todas las capas, pero centrándose en las capas 1, 2 y 3.

b. Examinar las funciones del plano de datos y del plano de control.

En los exámenes, recuerde que no obtendrá puntos extra por buenos métodos de resolución de problemas; por tanto, encuentre la respuesta de cualquier forma que pueda, aunque esto signifique que conjeture un poco basándose en el contexto de la pregunta. Por ejemplo, el proceso sugerido en el Paso 2A sugiere centrarse en las capas 1, 2 y 3; esta sugerencia está basada en el hecho de que los exámenes CCNA se centran principalmente en estas tres capas. Pero se debe atajar este proceso tanto como sea posible basándose en el enunciado de la pregunta.

Análisis de la causa raíz

El final de los tres pasos, el análisis de la causa raíz, se esfuerza por terminar el proceso de resolución de problemas identificando el dispositivo específico y la función que necesita ser reparada. La causa raíz es la verdadera razón de que el problema esté ocurriendo, y lo más importante, es la función que, cuando se arregle, solucionará este problema en particular.

Encontrar la causa raíz es de vital importancia porque la causa raíz, a diferencia de que se identifiquen muchos problemas en el proceso de aislamiento del problema, tiene una solución específica asociada con ella. Por ejemplo, continuando con el mismo problema de que R2 no puede enviar paquetes a PC2, considere la lista de problemas identificados a través del aislamiento del problema:

- R2 no puede enviar paquetes a PC2.
- R2 no recibe respuestas ARP de PC2.
- La interfaz de SW4 para el troncal con SW5 está en un estado *down*/*down*.
- El cable utilizado entre SW4 y SW5 utiliza una asignación incorrecta de pines en el cableado.

Todas estas declaraciones pueden ser ciertas en un escenario particular con problemas, pero sólo la última tiene una solución realizable obvia (reemplazar con un cable correcto). Mientras las otras declaraciones son válidas y se han encontrado hechos importantes durante el aislamiento del problema, no implican la acción específica a tomar para resolver el problema. Como resultado, el paso del análisis de la causa raíz se reduce a dos sencillas declaraciones:

Paso 1 Continuar aislando el problema hasta identificar la causa raíz, que a su vez tiene una solución obvia.

Paso 2 Si no puede reducir el problema a su verdadera causa raíz, aísle el problema lo más posible, y cambie algo en la red; esto probablemente cambiará los síntomas y le ayudará a identificar la causa raíz.

El mundo real frente a los exámenes

En el examen, puede buscar pistas en el tema general para el cual necesite aplicar alguna parte del proceso de resolución de problemas. Por ejemplo, si la figura muestra una red como la de la Figura 3.1, pero todas las respuestas multi-opción se refieren a VLANs y VTP, comience mirando el entorno LAN. Observe que aún podría querer considerar las capas 1 a 3, y los detalles del plano de datos y del plano de control, como ayuda para encontrar las respuestas.

Nota

Esta sección se aplica a la resolución de problemas de forma general, pero se incluye en este capítulo porque es el primer capítulo del libro dedicado a la resolución de problemas.

Resolución de problemas en el plano de datos de conmutación LAN

Las estrategias genéricas de resolución de problemas explicadas anteriormente en este capítulo sugieren comenzar con el proceso de envío IP en la capa 3. Si el ingeniero identifica un problema en un paso particular del proceso de envío IP, el siguiente paso debe ser examinar este paso del enrutamiento con más detalle, incluso mirando en el estado de las capas 1 y 2 subyacentes.

Las siguientes secciones examinan las herramientas y procesos utilizados en los procesos de resolución de problemas del plano de datos de LAN en las capas 1 y 2. El resto del capítulo asume que no existen problemas de capa 3; los capítulos 7 y 11 examinan la resolución de problemas de capa 3. Este capítulo también hace algunas referencias a protocolos del plano de control, en concreto VTP y el Protocolo de árbol de extensión (STP), pero VTP y STP ya han sido tratados en profundidad en los dos capítulos anteriores. Por tanto, estas secciones se centran especialmente en el plano de datos de la conmutación LAN.

Estas secciones comienzan con una revisión previa de los procesos de envío en switches LAN y una introducción a los cuatro pasos principales en los procesos de resolución de problemas de conmutación LAN sugeridos en este capítulo. Después, el texto examina sucesivamente cada uno de los cuatro pasos. Finalmente, se muestra un ejemplo de cómo aplicar el proceso de resolución de problemas.

Visión general del proceso de envío de conmutación LAN normal

El proceso de envío en los switches LAN, descrito en detalle en el Capítulo 7 del libro *CCENT/CCNA ICND1 Guía oficial para el examen de certificación*, es relativamente sencillo.

Sin embargo, antes de tener una visión más cercana de cómo utilizar la salida de los comandos show para predecir las operaciones normales y aislar la causa raíz de un problema de envío, resulta útil revisar cómo razona un switch en el proceso de envío cuando no existen problemas. Los siguientes pasos del proceso esbozan esta lógica:

Paso 1 Determinar la VLAN por la que debe enviarse la trama, como sigue:

- **a.** Si la trama llega por una interfaz de acceso, utilizar la VLAN de acceso de la interfaz.
- **b.** Si la trama llega por una interfaz troncal, utilizar la VLAN especificada en la cabecera de *trunking* de la trama.

Paso 2 Si la interfaz entrante está en un estado STP de Aprendizaje o Escucha en esa VLAN, añadir la dirección MAC de origen a la tabla de direcciones MAC, con la interfaz entrante y el ID VLAN (si no está ya en la tabla).

Paso 3 Si la interfaz entrante no está en un estado STP de Envío en esa VLAN, descartar la trama.

Paso 4 Buscar la dirección MAC de destino de la trama en la tabla de direcciones MAC, pero sólo para entradas en la VLAN identificada en el Paso 1. Si la MAC de destino se encuentra o no, seguir estos pasos:

- **a. Encontrada:** enviar la trama sólo por las interfaces listadas en la entrada encontrada de la tabla de direcciones.
- **b. No encontrada:** inundar la trama por todos los otros puertos de acceso en la misma VLAN que estén en un estado de Envío STP, y por todos los puertos troncales que incluyan esta VLAN como completamente soportada (activa, en la lista de permitidas, no recortada, envío STP).

Para enviar una trama, un switch debe determinar primero en qué VLAN será enviada (Paso 1), aprender las direcciones MAC de origen según sea necesario (Paso 2), y entonces elegir por dónde enviar la trama. Sólo para estar seguros de que el proceso está claro, considérese el ejemplo utilizado en la Figura 3.3, en el cual PC1 envía una trama a su router predeterminado, R1, con las direcciones MAC mostradas en la figura.

En este caso, se considera la trama enviada por PC1 (MAC de origen 0200.1111.1111) a R1 (MAC de destino 0200.0101.0101). SW1, usando el Paso 1 de la lógica resumida de envío, determina si la interfaz Fa0/11 está trabajando como una interfaz de acceso o de troncal. En este caso, es una interfaz de acceso asignada a la VLAN 3. Por el Paso 2, SW1 añade una entrada a su tabla de direcciones MAC, que contiene la dirección MAC 0200.1111.1111, la interfaz Fa0/11, y la VLAN 3. En el Paso 3, SW1 confirma que la interfaz entrante, Fa0/11, está en un estado de Envío STP. Finalmente, en el Paso 4, SW1 busca una entrada con la dirección MAC 0200.0101.0101 en VLAN 3. Si SW1 encuentra una entrada que especifica la interfaz Gigabit 0/1, SW1 enviará entonces la trama sólo por Gi0/1. Si la interfaz saliente (Gi0/1) es una interfaz troncal, SW1 añade una cabecera de *trunking* VLAN que especifica la VLAN 3, el ID VLAN determinado en el Paso 1.

Para examinar otro ejemplo ligeramente diferente, considere una difusión enviada por PC1. Los Pasos 1 hasta 3 ocurren como antes, pero en el Paso 4, SW1 inunda la

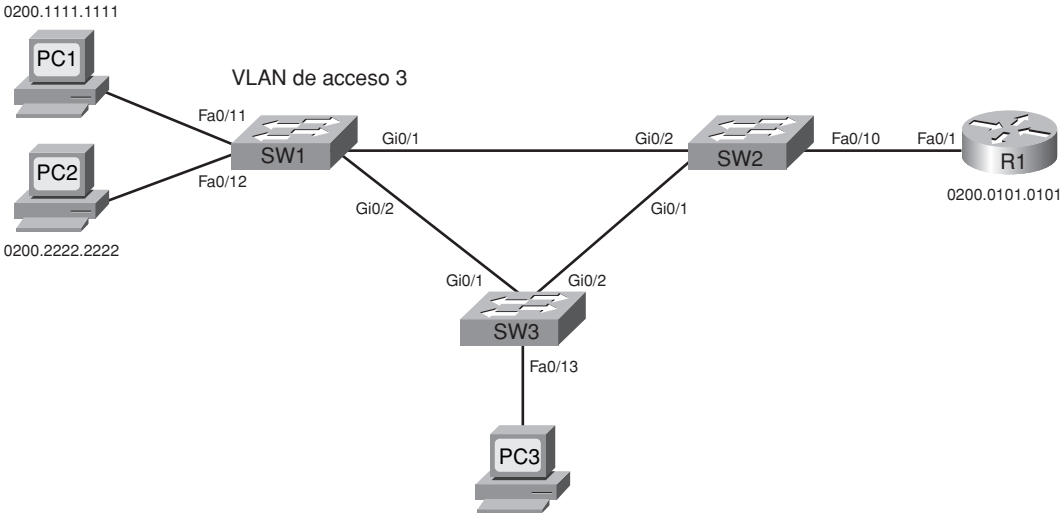


Figura 3.3. Red conmutada utilizada en el análisis del plano de datos en el Capítulo 3.

trama. Sin embargo, SW3 sólo inunda la trama por los puertos de acceso en VLAN 3 y puertos troncales que soporten a VLAN 3, con la restricción de que SW1 no enviará una copia de la trama por los puertos que no estén en un estado de Envío STP.

Aunque esta lógica de envío es relativamente sencilla, el proceso de resolución de problemas requiere de la aplicación de la mayoría de los conceptos relativos a las LANs de los libros ICND1 e ICND2, así como de otros temas. Por ejemplo, sabiendo que PC1 primero envía tramas a SW1, tiene sentido verificar el estado de la interfaz, para asegurarse de que la interfaz está "up/up", y arreglar el problema con la interfaz en caso contrario. Docenas de temas individuales podrían necesitar ser verificados en la resolución de un problema. Así, este capítulo sugiere un proceso de resolución de problemas del plano de datos LAN que organiza las acciones en cuatro pasos principales:

Paso 1 Confirmar los diagramas de red utilizando CDP.

Paso 2 Aislar los problema de interfaz.

Paso 3 Aislar los problemas de filtrado y seguridad de puerto.

Paso 4 Aislar los problemas de las VLANs y del *trunking*.

Las siguientes cuatro secciones revisan y explican los conceptos y las herramientas para realizar cada uno de estos cuatro pasos. Aunque algunos hechos e informaciones son nuevos, la mayoría de los conceptos específicos resaltados ya han sido tratados en *CCENT/CCNA ICND1 Guía oficial para el examen de certificación* o en los Capítulos 1 y 2 de este libro. El objetivo principal es ayudar a poner todos los conceptos juntos para analizar escenarios únicos (como se pedirá en los exámenes) empleando un poco menos de tiempo, con una muy buena posibilidad de éxito.

Nota

Las dos secciones siguientes, "Paso 1: confirmar los diagramas de red utilizando CDP" y "Paso 2: aislar los problemas de la interfaz", se tratan también en el Capítulo 10 del libro ICND1. Si está leyendo ambos libros para preparar el examen CCNA, no necesita leer estas secciones de este capítulo así como las secciones de nombre similar del Capítulo 10 de ICND1. Si está leyendo ambos libros, puede saltar a la sección "Paso 3: aislar los problemas de filtrado y de seguridad de puerto".

Paso 1: confirmar los diagramas de red utilizando CDP

El Protocolo de descubrimiento de Cisco (CDP, *Cisco Discovery Protocol*) puede ser útil para verificar la información del diagrama de red, así como para completar el resto de información necesaria sobre los dispositivos y la topología. En la vida real, los diagramas de red pueden ser viejos y estar anticuados, y se podría provocar un problema porque alguien mueve algunos cables y no actualiza los diagramas. Yo dudo que Cisco pudiera escribir una pregunta con información inexacta a propósito en la figura asociada con la pregunta, pero el examen puede incluir fácilmente preguntas para la que el diagrama de red no muestre toda la información necesaria, y sea necesario utilizar CDP para encontrar el resto de los detalles. Así, esta sección revisa CDP, y un primer buen paso de la resolución de problemas del plano de datos LAN es como sigue:

Paso 1 Verificar la exactitud y completar la información mostrada en el diagrama de red utilizando el comando CDP.

Nota

Este capítulo muestra una serie de pasos numerados para la resolución de problemas de conmutación LAN, empezando aquí con el Paso 1. Los pasos y sus números no son importantes para el examen; los pasos están numerados en este capítulo sólo a título orientativo.

Los routers, switches y otros dispositivos de Cisco utilizan CDP por varias razones, pero los routers y los switches lo utilizan para anunciar la información básica acerca de ellos mismos a sus vecinos (información como el nombre del elemento, tipo de dispositivo, versión del IOS y números de interfaz). Tres comandos en particular muestran la información CDP aprendida de sus vecinos, como se indica en la Tabla 3.1. De hecho, en los casos en los que no exista diagrama, un ingeniero puede crear un diagrama de routers y switches utilizando la salida del comando `show cdp`.

La única parte con truco del proceso de comparación de la salida CDP con un diagrama es que la salida muestra dos interfaces o puertos en muchas líneas de la salida. Leyendo de izquierda a derecha, la salida normalmente presenta el nombre de host del dispositivo vecino bajo el título "Device ID". Sin embargo, el siguiente título, "Local Intrfce", que significa

Tabla 3.1. Comandos que listan información acerca de los vecinos.

Comando	Descripción
show cdp neighbors [*tipo número*]	Muestra una línea de resumen con información acerca de cada vecino, o del vecino encontrado en una interfaz concreta si se especifica en el comando.
show cdp neighbors detail	Muestra un conjunto grande de información (aproximadamente 15 líneas), para cada vecino.
show cdp entry *nombre*	Muestra la misma información que el comando show cdp neighbors detail, pero sólo para el vecino especificado.

"interfaz local", es el nombre/número de la interfaz local del dispositivo. El nombre/número de interfaz del dispositivo vecino está en el lado derecho de la salida del comando bajo el título "Port ID". El Ejemplo 3.1 muestra un ejemplo del comando show cdp neighbors desde SW2 en la Figura 3.3. Tómese un tiempo en comparar las partes sombreadas de la salida del comando con los detalles concretos de la Figura 3.3 para ver qué campos listan interfaces de cada dispositivo.

Ejemplo 3.1. Ejemplo del comando **show cdp**.

```
SW2#show cdp neighbors
Capability Codes: R - Router,  T - Trans Bridge,  B - Source Route Bridge
                  S - Switch,  H - Host, I - IGMP, r - Repeater, P - Phone

Device ID      Local Intrfce  Holdtme        Capability     Platform       Port ID
SW1            Gig 0/2        173            S I            WS-C2960-2     Gig 0/1
R1             Fas 0/10       139            R S I          1841           Fas 0/1
```

CDP produce una exposición de seguridad cuando se habilita. Para evitar la exposición de permitir a un atacante aprender detalles acerca de cada switch, CDP puede ser fácilmente deshabilitado. Cisco recomienda que CDP esté deshabilitado en todas las interfaces que no tengan una necesidad específica de él. Las interfaces que con más probabilidad necesiten utilizar CDP son las interfaces conectadas a otros routers y switches de Cisco y las interfaces conectadas a teléfonos IP de Cisco. Por otra parte, CDP puede ser deshabilitado en una interfaz utilizando el subcomando de interfaz no cdp enable. (El subcomando de interfaz cdp enable rehabilita CDP.) Alternativamente, el comando global no cdp run deshabilita CDP en el switch entero; el comando global cdp run rehabilita CDP globalmente.

Paso 2: aislar los problemas de interfaz

Una interfaz de un switch de Cisco debe estar funcionando antes de que el switch pueda procesar las tramas recibidas por la interfaz o enviar tramas por la interfaz. Por tanto,

un paso obvio de la resolución de problemas debe ser examinar el estado de cada interfaz, especialmente los que se espera utilizar cuando se reenvían tramas, y verificar que las interfaces están en estado "up" y funcionando.

Esta sección examina los estados posibles de una interfaz en un switch basado en el IOS de Cisco, muestra las causas raíz de los estados no operacionales, y trata un problema muy común que ocurre aun cuando la interfaz parece estar en un estado operativo. Las tareas específicas para este paso se pueden resumir con los siguientes pasos de resolución de problemas:

Paso 2 Verificar los problemas de interfaz como sigue:

- **a.** Determinar el(los) código(s) de estado de interfaz para cada interfaz requerida, y si no está en un estado conectado (*connect*) o *up/up*, resolver los problemas hasta que la interfaz alcance el estado conectado (*connect*) o *up/up*.
- **b.** Para una interfaz en un estado conectado (*connect*) o *up/up,* verificar también otros dos problemas: desigualdad de dúplex y algunas variaciones de seguridad de puerto que desechan las tramas a propósito.

Códigos de estado de interfaz y razones de los estados no operativos

Los switches Cisco utilizan dos conjuntos diferentes de códigos de estado: un conjunto de dos códigos (palabras) que utilizan la misma convención que en los códigos de estado de interfaz de un router y otro conjunto con un solo código (palabra). Ambos conjuntos de códigos de estado pueden determinar si una interfaz está funcionando.

Los comandos de switch show interfaces y show interfaces description muestran el estado de dos códigos igual que los routers. Los dos códigos se llaman **estado de la línea** y **estado del protocolo**, e indican si la capa 1 está funcionando y si la capa 2 está funcionando, respectivamente. Las interfaces de switch LAN muestran normalmente una interfaz con ambos códigos como "up" o ambos códigos como "down", debido a que todas las interfaces de switch utilizan los mismos protocolos de capa de enlace de datos Ethernet, por lo que el protocolo de capa de enlace de datos nunca debe tener un problema.

Nota

Este libro se refiere a estos dos códigos de forma abreviada con una barra entre ellos, por ejemplo, "up/up".

El comando show interfaces status muestra un único código de estado de interfaz. Este único código de estado de interfaz se corresponde con diferentes combinaciones de los códigos de estado de interfaz tradicionales de dos códigos y puede ser fácilmente correlacionado con estos códigos. Por ejemplo, el comando show interfaces status lista un estado "connect" para las interfaces que funcionan, que se corresponde con el estado up/up que se muestra en los comandos show interfaces y show interfaces description.

Cualquier otro estado de interfaz diferente a conectado o up/up significa que el switch no puede enviar o recibir tramas por la interfaz. Cada interfaz en estado no operativo tiene un conjunto pequeño de causas raíz. También, observe que los exámenes podrían formular una pregunta que sólo muestre uno u otro tipo de código de estado; por tanto, para estar preparado para los exámenes, debe conocer el significado de ambos conjuntos de códigos de estado de interfaz. La Tabla 3.2 presenta las combinaciones de código y algunas causas raíz que podrían haber provocado un estado particular de interfaz.

Tabla 3.2. Códigos de estado de interfaz de switch LAN.

Estado de línea	Estado de protocolo	Estado de interfaz	Causa raíz principal
Admin. down	down	disabled	La interfaz se ha configurado con el comando shutdown.
down	down	notconnect	Sin cable; cable dañado; conexión errónea de los pines del cable; velocidades no coincidentes en los dos dispositivos conectados; el dispositivo del otro extremo del cable está apagado o la otra interfaz no se halla en un estado operativo.
up	down	notconnect	No esperado en interfaces de switch LAN.
down	down (err-disabled)	err-disabled	La seguridad de puerto ha deshabilitado la interfaz.
up	up	connect	La interfaz está funcionando.

El estado notconnect y las especificaciones de cableado

La Tabla 3.2 muestra varias razones por las que una interfaz de switch puede estar en estado desconectado. La mayoría de estas razones no necesitan mucha más explicación que la que el texto da en la tabla. Por ejemplo, si una interfaz está conectada a otro switch, y la interfaz está en un estado no conectado, comprobar el otro switch para ver si su interfaz ha sido cerrada. Sin embargo, una de las razones para el estado no conectado (incorrecta conexión de los pines del cable) merece un poco más de atención porque es un error común y no se trata en ninguna otra parte de este libro. (La conexión de los pines de los cables Ethernet se trata en el Capítulo 3 del libro *CCENT/CCNA ICND1*.)

Los estándares de cableado Ethernet de par trenzado sin apantallar (UTP, *unshielded twisted-pair*) especifica los pines que se deben conectar en los conectores RJ-45 de los dos extremos del cable. Los dispositivos transmiten utilizando pares de cables. 10BASE-T y 100BASE-Tx utilizan dos pares: uno para transmitir y otro para recibir datos. Cuando se conectan dos dispositivos que utilizan el mismo par de pines para transmitir, el cable (un cable cruzado) debe conectar o cruzar los cables del par del dispositivo que transmite con el par del dispositivo receptor esperado. Recíprocamente, los dispositivos que ya usen pares opuestos para transmitir datos necesitan un cable recto que no cruce los pares. La Figura 3.4 muestra un ejemplo en una típica LAN conmutada, donde se muestran los tipos de conexiones de los cables.

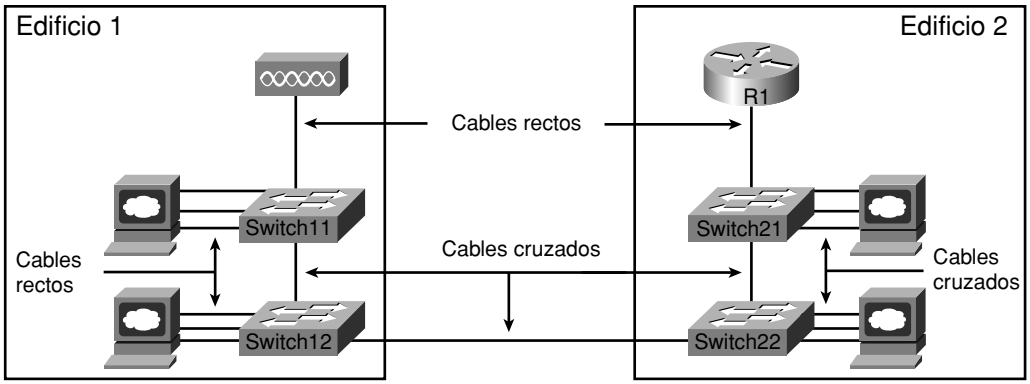


Figura 3.4. Ejemplo del uso de cables cruzados y rectos.

Una resolución de problemas efectiva requiere tener conocimiento de los pares por los que los dispositivos transmiten. La Tabla 3.3 lista los dispositivos más comunes vistos en el contexto de CCNA, junto con los pares utilizados. Observe que cuando se conectan dos tipos de dispositivos de la misma columna, se necesita un cable cruzado; cuando se conectan dos dispositivos de diferente columna de la tabla, se necesita un cable recto.

Tabla 3.3. Pares de pines utilizados en 10 BASE-T y 100 BASE-Tx.

Dispositivos que transmiten por 1,2 y reciben por 3,6	**Dispositivos que transmiten por 3,6 y reciben por 1,2**
Tarjetas de red (NIC) de PC	Hubs
Routers	Switches
Puntos de acceso inalámbricos (interfaz Ethernet)	—
Impresoras de red conectadas a Ethernet	—

Velocidad de la interfaz y problemas con dúplex

Las interfaces de los switches pueden encontrar sus valores de velocidad y dúplex de varias maneras. De forma predeterminada, las interfaces que utilizan cables de cobre y son capaces de establecer varias velocidades y dúplex utilizan el proceso de autonegociación estándar del IEEE (IEEE 802.3x). Alternativamente, las interfaces de switches, routers y la mayoría de las tarjetas de interfaz de red (NIC) también pueden ser configurados para utilizar una velocidad específica o dúplex. En switches y routers, el subcomando de interfaz speed {10 | 100 | 1000} con el subcomando de interfaz duplex {half | full} establecen estos valores. Tenga en cuenta que configurando velocidad y dúplex en una interfaz de switch deshabilita el proceso estándar de negociación del IEEE en esa interfaz.

Los comando show interfaces y show interfaces status muestran ambos los valores de velocidad y dúplex establecidos en una interfaz, como se muestra en el Ejemplo 3.2.

Ejemplo 3.2. Visualización de los valores de velocidad y dúplex en las interfaces de switch.

```
SW1#show interfaces status

Port    Name      Status         Vlan       Duplex   Speed   Type
Fa0/1             notconnect     1          auto     auto    10/100BaseTX
Fa0/2             notconnect     1          auto     auto    10/100BaseTX
Fa0/3             notconnect     1          auto     auto    10/100BaseTX
Fa0/4             connected      1          a-full   a-100   10/100BaseTX
Fa0/5             connected      1          a-full   a-100   10/100BaseTX
Fa0/6             notconnect     1          auto     auto    10/100BaseTX
Fa0/7             notconnect     1          auto     auto    10/100BaseTX
Fa0/8             notconnect     1          auto     auto    10/100BaseTX
Fa0/9             notconnect     1          auto     auto    10/100BaseTX
Fa0/10            notconnect     1          auto     auto    10/100BaseTX
Fa0/11            connected      1          a-full   10      10/100BaseTX
Fa0/12            connected      1          half     100     10/100BaseTX
Fa0/13            connected      1          a-full   a-100   10/100BaseTX
Fa0/14            disabled       1          auto     auto    10/100BaseTX
Fa0/15            notconnect     3          auto     auto    10/100BaseTX
Fa0/16            notconnect     3          auto     auto    10/100BaseTX
Fa0/17            connected      1          a-full   a-100   10/100BaseTX
Fa0/18            notconnect     1          auto     auto    10/100BaseTX
Fa0/19            notconnect     1          auto     auto    10/100BaseTX
Fa0/20            notconnect     1          auto     auto    10/100BaseTX
Fa0/21            notconnect     1          auto     auto    10/100BaseTX
Fa0/22            notconnect     1          auto     auto    10/100BaseTX
Fa0/23            notconnect     1          auto     auto    10/100BaseTX
Fa0/24            notconnect     1          auto     auto    10/100BaseTX
Gi0/1             connected      trunk      full     1000    10/100/1000BaseTX
Gi0/2             notconnect     1          auto     auto    10/100/1000BaseTX
SW1#show interfaces fa0/13
```

(continúa)

Ejemplo 3.2. Visualización de los valores de velocidad y dúplex en las interfaces de switch *(continuación).*

```
FastEthernet0/13 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0019.e86a.6f8d (bia 0019.e86a.6f8d)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
   reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:05, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
   85022 packets input, 10008976 bytes, 0 no buffer
   Received 284 broadcasts (0 multicast)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 281 multicast, 0 pause input
   0 input packets with dribble condition detected
   95226 packets output, 10849674 bytes, 0 underruns
   0 output errors, 0 collisions, 1 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 PAUSE output
   0 output buffer failures, 0 output buffers swapped out
```

Aunque ambos comandos pueden ser útiles, sólo el comando show interfaces status muestra cómo el switch determina los valores de velocidad y dúplex. La salida del comando muestra los valores negociados con una "a-". Por ejemplo, "a-full" significa full-dúplex autonegociado, mientras que "full" significa full-dúplex pero configurado manualmente. El ejemplo sombrea la salida del comando que muestra que la velocidad y dúplex de la interfaz Fa0/12 del switch no fueron autonegociados, pero Fa0/13 utiliza la autonegociación. Observe que el comando show interfaces Fa0/13 (sin la opción status) simplemente lista la velocidad y el dúplex para la interfaz Fa0/13, con nada que implique que los valores fueron aprendidos mediante autonegociación.

Los switches de Cisco tienen algunas características interesantes relativas a la velocidad de la interfaz que pueden ayudar a determinar algunos tipos de problemas de interfaz. Si una interfaz de un switch de Cisco se ha configurado a una velocidad en particular, y la velocidad no coincide con la del dispositivo del otro extremo del cable, la interfaz del switch podría estar en un estado no conectado o down/down. Sin embargo, esta clase de desigualdades sólo pueden ocurrir cuando la velocidad ha sido manualmente configurada en el switch. Las interfaces de los switches de Cisco que no han sido configuradas con el comando speed pueden detectar automáticamente la velocidad utilizada por el otro dis-

positivo (incluso si el otro dispositivo deshabilita el proceso de autonegociación de IEEE) y entonces utilizar esa velocidad.

Por ejemplo, en la Figura 3.3, imagine que la interfaz Gi0/2 de SW2 fue configurada con los comandos speed 100 y duplex half (no recordando los valores para una interfaz Gigabit, por cierto). SW2 podría utilizar estos valores y deshabilitar el proceso de autonegociación estándar del IEEE porque los comandos speed y duplex han sido configurados. Si la interfaz Gi0/1 de SW1 no tiene un comando speed configurado, SW1 podría todavía reconocer la velocidad (100 Mbps) —incluso aunque SW2 podría no usar la autonegociación estándar del IEEE— y SW1 podría también utilizar una velocidad de 100 Mbps. El Ejemplo 3.3 muestra los resultados de este caso específico en SW1.

Ejemplo 3.3. Mostrando los valores de velocidad y dúplex en las interfaces de switch.

```
SW1#show interfaces gi0/1 status

Port    Name      Status          Vlan        Duplex    Speed   Type
Gi0/1             connected       trunk       a-half    a-100   10/100/1000BaseTX
```

La velocidad y dúplex todavía se muestran con el prefijo "a-" en este ejemplo, lo que implica la autonegociación. La razón es que en este caso, la velocidad se estableció automáticamente, y el valor dúplex fue elegido porque es el valor predeterminado utilizado por el proceso de autonegociación del IEEE. El estado estándar del IEEE para puertos de 100 Mbps, si la autonegociación falla, utiliza una configuración semidúplex predeterminada.

Encontrar una desigualdad de dúplex puede ser mucho más difícil que encontrar una desigualdad de velocidad porque *si los valores de dúplex no coinciden en los extremos de un segmento Ethernet, la interfaz del switch estará en un estado conectado (up/up)*. En este caso, la interfaz funciona, pero podría funcionar pobremente, con un rendimiento pobre y con síntomas de problemas intermitentes. La razón es que el dispositivo utiliza semidúplex usando la lógica de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD, *carrier sense multiple access collision detect)*, esperando para enviar cuando recibe una trama, creyendo que puede haber colisiones cuando no es posible físicamente, y dejando de enviar una trama porque el switch cree que ocurre una colisión. Con una carga de tráfico suficiente, la interfaz podrá estar en un estado conectado, pero esencialmente inutilizable para pasar tráfico, causando incluso la pérdida de mensajes vitales de VTP y STP.

Para identificar problemas de desigualdad de dúplex, realice las siguientes acciones:

- Utilice comandos como show interfaces en cada extremo del enlace para confirmar el valor dúplex en cada uno.
- Busque el incremento de ciertos contadores en las interfaces semidúplex. Los contadores (*runts*, colisiones y últimas colisiones) ocurren cuando el otro dispositivo utiliza full dúplex. (Observe que estos contadores también pueden incrementarse cuando se producen colisiones legítimas.)

El Ejemplo 3.2 (anteriormente en esta sección) muestra sombreados estos contadores en la salida del comando show interfaces.

La causa raíz de las desigualdades de dúplex puede estar relacionada con los valores predeterminados elegidos por el proceso de autonegociación IEEE. Cuando un dispositivo intenta autonegociar, y el otro no responde, el primero elige el valor predeterminado de duplex basándose en la velocidad actual. La configuración dúplex predeterminada, para el IEEE, se selecciona como sigue:

- Si la velocidad es de 10 ó 100 Mbps, utilizar como valor predeterminado semidúplex.
- Si la velocidad es 1000 Mbps, utilizar como valor predeterminado full-dúplex (dúplex).

Nota

Las interfaces de Ethernet mayores de 1 Gbps siempre utilizan full-dúplex.

Paso 3: aislar los problemas de filtrado y de seguridad de puerto

Hablando de forma general, cualquier análisis del proceso de envío debería considerar cualquier característica de seguridad que pudiera descartar algunas tramas o paquetes. Por ejemplo, los routers y los switches pueden configurarse con listas de control de acceso (ACL, *access control lists*) que examinan los paquetes y tramas enviados y recibidos por una interfaz, con el router o switch descartando esos paquetes/tramas.

Los exámenes CCNA no tratan el tema de las ACLs de switch, pero sí una característica similar llamada seguridad de puerto. Como se trata en el Capítulo 9 del libro *CCENT/CCNA ICND1*, la característica de seguridad de puerto puede utilizarse para hacer que el switch descarte algunas tramas enviadas por o hacia una interfaz. La seguridad de puerto tiene tres características básicas con la cuales determina qué tramas filtrar:

- Limita qué direcciones MAC específicas pueden enviar y recibir tramas en una interfaz de switch, descartando tramas hacia/desde otras direcciones MAC.
- Limita el número de direcciones MAC usando la interfaz, descartando tramas hacia/desde direcciones MAC aprendidas después de alcanzar el límite máximo.
- Una combinación de los dos puntos anteriores.

El primer paso para resolver los problemas relacionados con la seguridad de puerto debe ser encontrar qué interfaces tienen la seguridad de puerto habilitada, seguido de una determinación de si está ocurriendo alguna violación. La parte más extraña está relacionada con las diferentes reacciones del IOS cuando se produce una violación basándose en el subcomando de interfaz switchport port-security violation *modo-violación*, que le dice al switch qué hacer cuando ésta ocurre. El proceso general es como sigue:

Paso 3 Verificar problemas de seguridad de puerto como sigue:

a. Identificar todas las interfaces en las que se ha habilitado la seguridad de puerto (show running-config o show port-security).

b. Determinar si está ocurriendo una violación de seguridad basándose en la parte *modo-violación* de la configuración de seguridad de puerto de la interfaz, como sigue:

- shutdown: la interfaz estará en un estado *err-disabled*.
- restrict: la interfaz estará en un estado conectado, pero el comando show port-security interface mostrará un incremento del contador de violaciones.
- protect: la interfaz estará en un estado conectado, y el comando show port-security interface no mostrará ahora un incremento del contador de violaciones.

c. En todos los casos, comparar la configuración de la seguridad de puerto con el diagrama, así como con el campo "last source address" en la salida del comando show port-security interface.

Una de las dificultades en la resolución de problemas de seguridad de puerto está relacionada con el hecho de que algunas configuraciones de seguridad de puerto sólo descartan las tramas ofensoras, pero no deshabilitan la interfaz como resultado, todo basado en el modo de violación configurado. Los tres modos de violación descartan el tráfico como se especifica en la configuración. Por ejemplo, si sólo está permitida la dirección MAC predefinida 0200.1111.1111, el switch descarta todo el tráfico por esa interfaz, que no llegue o salga de 0200.1111.1111. Sin embargo, el modo *shutdown* provoca que todo el tráfico futuro se descarte (incluso el tráfico legítimo de la dirección 0200.1111.1111) después de que ocurra una violación. La Tabla 3.4 resume algunos de estos puntos clave para facilitar su estudio.

Tabla 3.4. Comportamiento de la seguridad de puerto basada en el modo de violación.

Modo de violación	Descarta tramas ofensivas	Descarta todo el tráfico después de la violación	La violación resulta en un estado de la interfaz de *err-disabled*	Incremento de contadores por cada nueva violación
shutdown	Sí	Sí	Sí	Sí
restrict	Sí	No	No	Sí
protect	Sí	No	No	No

El Paso 3B de la resolución de problemas se refiere al estado de interfaz *err-disabled* (error deshabilitado). Este estado verifica que la interfaz ha sido configurada para usar la seguridad de puerto, que ha ocurrido una violación, y que en este momento no se permite tráfico en la interfaz. Este estado de interfaz implica que se está utilizando el modo *shutdown* de violación, porque es el único de los tres modos de seguridad de puerto que provoca la inhabilitación de la interfaz. Para solucionar este problema, la interfaz debe ser cerrada y después habilitada con los comandos shutdown y no shutdown. El Ejemplo 3.4 muestra un ejemplo en el cual una interfaz está en el estado *err-disabled*.

Ejemplo 3.4. Utilizando la seguridad de puerto para definir direcciones MAC correctas en interfaces particulares.

```
! El primer comando muestra todas las interfaces en las cuales ha sido habilitada
! la seguridad de puerto, y el modo de violación, bajo el título "Security Action".
SW1#show port-security
Secure Port    MaxSecureAddr   CurrentAddr   SecurityViolation  Security Action
                   (Count)       (Count)          (Count)
---------------------------------------------------------------------------
    Fa0/13              1             1                   1       Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8320
!
! El siguiente comando muestra el estado err.disable, lo que implica
! una violación de seguridad.
SW1#show interfaces Fa0/13 status

Port       Name        Status       Vlan         Duplex  Speed   Type
Fa0/13                 err-disabled 1            auto    auto    10/100BaseTX
!
! La salida del siguiente comando tiene sombreados algunos de los datos
! más importantes.
SW1#show port-security interface Fa0/13
Port Security                  : Enabled
Port Status                    : Secure-shutdown
Violation Mode                 : Shutdown
Aging Time                     : 0 mins
Aging Type                     : Absolute
SecureStatic Address Aging     : Disabled
Maximum MAC Addresses          : 1
Total MAC Addresses            : 1
Configured MAC Addresses       : 1
Sticky MAC Addresses           : 0
Last Source Address:Vlan       : 0200.3333.3333:2
Security Violation Count       : 1
```

La salida del comando show port-security interface muestra un par de elementos útiles en el proceso de resolución de problemas. El estado de puerto Secure-shutdown significa que la interfaz esta deshabilitada para todo el tráfico como resultado de una violación, y que el estado de la interfaz debe ser *err-disabled*. El final de la salida del comando muestra el contador de violaciones, incrementándose en 1 por cada nueva violación. De forma interesante, con un modo de violación de *shutdown*, el contador se incrementa en 1, la interfaz se coloca en el estado *err-disabled*, y el contador no se incrementará de nuevo hasta que el ingeniero utilice los comandos shutdown y no shutdown en la interfaz, en este orden. Finalmente, observe que las dos últimas líneas muestran la dirección MAC de origen de la última trama recibida en la interfaz. Este valor puede ser útil para identificar la dirección MAC del dispositivo que causa la violación.

Los modos de violación restringido (*restrict*) y protegido (*protect*) también causan el descarte de tramas, pero con un comportamiento diferente. Con estos modos de violación, la interfaz permanece en estado conectado (*up/up*) mientras sigue descartando tramas inapropiadas debido a la seguridad de puerto. Por tanto, evite la trampa de asumir que una interfaz en un estado conectado, o *up/up*, no pueda tener otras razones para no pasar tráfico.

El Ejemplo 3.5 muestra un ejemplo de configuración y el comando show cuando se utiliza el modo protegido (*protect*). En este caso, un PC con la dirección MAC 0200.3333.3333 envía tramas por el puerto Fa0/13, con el puerto configurado para restringir Fa0/13 para recibir sólo tramas enviadas por 0200.1111.1111.

Ejemplo 3.5. Seguridad de puerto utilizando el modo protegido.

```
SSW1#show running-config
! Se han omitido líneas para abreviar
interface FastEthernet0/13
switchport mode access
switchport port-security
switchport port-security mac-address 0200.1111.1111
switchport port-security violation protect
! Se han omitido líneas para abreviar
SW1#show port-security interface Fa0/13
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0200.3333.3333:1
Security Violation Count   : 0
```

Esta salida del comando show fue tomada antes de que muchas tramas fueran enviadas por un PC con la dirección MAC 0200.3333.3333, con todas las tramas siendo descartadas por el switch debido a la seguridad de puerto. La salida del comando muestra la dirección MAC no permitida del PC 0200.3333.3333 como la última dirección MAC de origen de una trama recibida. Sin embargo, observe que el estado del puerto es mostrado como Secure-up y el contador de violación está a 0 (ambas indicaciones podrían hacer pensar que todo va bien). Sin embargo, en modo protegido, el comando show port-security interface no muestra ninguna información que confirme que ha habido una violación. La única indicación es que el tráfico del usuario final no llega hasta donde debería.

Si en este ejemplo se hubiera utilizado el modo restringido (*restrict*), el estado del puerto también sería *secure-up*, pero el contador de violaciones de seguridad se incrementaría en uno por cada trama que viole las restricciones de seguridad.

Para los exámenes, una violación de la seguridad de puerto podría no ser un problema; podría ser la función exacta pensada. El texto de la pregunta podría establecer explícitamente qué seguridad de puerto debe realizarse. En estos casos, busque los datos de configuración de la seguridad de puerto. Después, compare la configuración con las direcciones MAC de los dispositivos conectados a la interfaz. El problema más parecido en los exámenes es que las direcciones MAC hayan sido mal configuradas o que el máximo número de direcciones MAC se haya establecido a un valor demasiado bajo. (El Capítulo 9 del libro *CCENT/CCNA ICND1*, explica los detalles de las sentencias de configuración.)

Una última característica que necesita una breve mención es la autenticación IEEE 802.1x. IEEE 802.1x (no confundir con el estándar IEEE 802.3x de autonegociación) define el proceso para autenticar al usuario del PC conectado a un puerto de switch. 802.1x puede ser utilizado como parte de una estrategia general de Control de admisión de red (NAC, *Network Admission Control*), en la cual el usuario interno de una LAN empresarial no puede utilizar la LAN hasta haber proporcionado alguna credencial de autenticación.

Con 802.1x, cada usuario se comunica con un servidor AAA con una serie de mensajes de autenticación. El switch de acceso escucha estos mensajes, descartando todas las tramas del enlace excepto los mensajes 802.1x a y desde el PC. Cuando el switch escucha por casualidad el mensaje desde el servidor AAA que dice que el usuario ha sido autenticado con éxito, el switch entonces permite todo el tráfico que circula por ese puerto. Si el usuario no es autenticado, el switch no permite tráfico en esta interfaz. Los detalles de cómo configurar 802.1x, y reconocer un fallo de autenticación como la causa raíz de un problema particular, queda fuera del alcance de este libro.

Paso 4: Aislar problemas de VLAN y de *trunking*

El proceso de envío de un switch depende de las definiciones de las VLANs de acceso en las interfaces de acceso y en los troncales VLAN que pueden pasar tráfico de muchas VLANs. Además, antes de que un switch pueda enviar tramas de una VLAN particular, el switch debe conocerla, bien por configuración o bien por VTP, y la VLAN debe estar activa. Las siguientes secciones examinan algunas de las herramientas con respecto a estos temas relativos a VLAN. Este paso de configuración incluye los siguientes pasos:

Paso 4 Verificar las VLANs y los troncales VLAN como sigue:

- **a.** Identificar todas las interfaces de acceso y sus VLANs de acceso asignadas, y reasignar a las VLANs correctas si es necesario.
- **b.** Determinar si las VLANs existen (configuradas o aprendidas con VTP) y están activas en cada switch. Si no, configurar y activar las VLANs para resolver el problema como sea necesario.
- **c.** Identificar las interfaces de *trunking* operativas en cada switch, y determinar las VLANs que se pueden enviar por cada troncal.

Las tres secciones siguientes tratan sucesivamente los pasos 4A, 4B y 4C.

Asegurarse de que las interfaces de acceso correctas están en las VLANs correspondientes

Para asegurar que cada interfaz de acceso ha sido asignada a la VLAN correcta, los ingenieros sólo tienen que determinar qué interfaces de switch son interfaces de acceso en vez de interfaces troncales, determinar las VLANs de acceso asignadas en cada interfaz, y comparar la información con la documentación. Los tres comandos show listados en la Tabla 3.5 pueden ser particularmente útiles en este proceso.

Tabla 3.5. Comandos que pueden encontrar puertos de acceso y VLANs.

Comando EXEC	Descripción
show vlan brief show vlan	Lista cada VLAN y todas las interfaces asignadas a esta VLAN, pero no incluye los troncales.
show interfaces *tipo número* switchport	Identifica la VLAN de acceso de una interfaz, la VLAN de voz, y el modo administrativo (configurado) y el modo operativo (acceso o troncal).
show mac address-table dynamic	Lista entradas de la tabla MAC: direcciones MAC con interfaces asociadas y VLANs.

Si es posible, empezar este paso con los comandos show vlan y show vlan brief, porque muestran todas las VLANs conocidas y las interfaces de acceso asignadas a cada VLAN. Sea consciente, no obstante, de que la salida de estos comandos incluye todas las interfaces que actualmente no forman un troncal operativo. Por tanto, estos comandos listan interfaces en estado no conectado, estado *err-disabled*, y lo más importante en este caso, interfaces que podrían formar un troncal después de que la interfaz se active. Por ejemplo, estos comandos podrían incluir a la interfaz Gi0/2 en la lista de interfaces en la VLAN 1, pero tan pronto como Gi0/1 se active, la interfaz podría negociar el *trunking* (en este punto, la interfaz no sería más una interfaz de acceso y no aparecería en la salida del comando show vlan brief).

Si los comandos show vlan y show interface switchport no están disponibles en una pregunta particular de test, el comando show mac address-table también puede ayudar a identificar la VLAN de acceso. Este comando lista la tabla de direcciones MAC, con cada entrada incluyendo una dirección MAC, la interfaz, y el ID VLAN. Si la pregunta de test implica que una interfaz de switch conecta a un único dispositivo PC, sólo verá una entrada en la tabla MAC que lista esa interfaz de acceso particular; el ID VLAN listado para esa misma entrada identifica la VLAN de acceso. (No se pueden hacer tales afirmaciones para interfaces troncales).

Después de determinar las interfaces de acceso y las VLANs asociadas, si la interfaz está asignada a la VLAN equivocada, utilice el subcomando de interfaz switchport access vlan *id-vlan* para asignar el ID VLAN correcto.

Las VLANs de acceso no se están definiendo o no están activadas

El siguiente paso de la resolución de problemas, Paso 4B, examina el hecho de que un switch no reenvía tramas en una VLAN no definida o en una definida que no está en estado activo. Esta sección resume la mejor manera de confirmar que un switch conoce que una VLAN particular existe, y si existe, determinar el estado de la VLAN.

Los servidores y clientes VTP sólo muestran su lista actual de VLANs conocidas con el comando show vlan. Ni el fichero de configuración en ejecución (*running-config*) ni el fichero de configuración de arranque (*startup-config*) contienen los comandos de configuración global vlan *id-vlan* que definen la VLAN, o los comandos name asociados que dan nombre a una VLAN. Los switches en modo transparente guardan estos comandos de configuración en el fichero vlan.dat y en el fichero *running-config*, por lo que la configuración se puede ver utilizando el comando show running-config.

Después de determinar que una VLAN no existe, el problema puede ser simplemente que la VLAN necesita ser definida. Si es así, siga el proceso de configuración de VLAN como se trató en detalle en el Capítulo 1, resumido a continuación:

- **En servidores y clientes VTP, asumiendo que VTP está funcionando**. La VLAN debe configurarse en un servidor VTP, típicamente con el comando global de configuración vlan *id-vlan*, con los otros servidores y clientes aprendiendo acerca de la VLAN. La VLAN puede configurarse también con el subcomando de interfaz switchport access vlan *id-vlan*, en el servidor VTP en el que la VLAN no existe todavía, provocando que el servidor cree automáticamente la VLAN.
- **En servidores y clientes VTP, asumiendo que VTP no funciona**. Resuelva el problema de VTP como se trata en la sección "Resolución de problemas de VTP" del Capítulo 1.
- **En un switch transparente VTP**. La configuración es la misma que en un servidor, pero debe ser hecha en cada switch, porque los switches en modo transparente VTP no publican la nueva VLAN a los otros switches.

Para cualquier VLAN existente, verificar también que la VLAN está activa. El comando show vlan puede listar uno de dos valores de estado de VLAN: activo (*active*) y *act/lshut*. El segundo de estos estados significa que la VLAN está cerrada. Para resolver este problema, utilizar el comando de configuración global no shutdown vlan *id-vlan*. Observe que este comando debe ser ejecutado en cada switch, porque este estado *shutdown* no es publicado por VTP.

Identificar los troncales y las VLANs enviadas en esos troncales

En este paso (4C), debe separar los problemas en dos categorías generales para comenzar a aislar el problema: problemas con los detalles de cómo un troncal operativo funciona y problemas causados cuando una interfaz que debe ser troncal no lo es.

La primera categoría en este paso puede ser hecha fácilmente utilizando el comando show interfaces trunk, que sólo muestra información acerca de los troncales operativos actualmente. El mejor lugar para comenzar con este comando es la última sección de la salida, que presenta las VLANs cuyo tráfico será enviado por el troncal. Cualquier VLAN que hace esto en su lista final de VLANs en la salida del comando aplica los siguientes criterios:

- La VLAN existe y está activa en este switch (como se ha tratado en la sección previa y puede verse en el comando show vlan).
- La VLAN no ha sido eliminada de la lista de VLANs permitidas en el troncal (como se configura con el subcomando de interfaz switchport trunk allowed vlan).
- La VLAN no ha sido recortada por VTP (*VTP-pruned*) del troncal (como hace automáticamente VTP, asumiendo que el *pruning* VTP ha sido habilitado con el comando de configuración global vtp pruning).
- El troncal está en un estado de Envío de STP en esa VLAN (como también puede verse con el comando show spanning-tree vlan *id-vlan*).

El Ejemplo 3.6 muestra un ejemplo de la salida del comando show interfaces trunk, con la sección final sombreada. En este caso, el troncal sólo envía tráfico de las VLANs 1 y 4.

Ejemplo 3.6. Lista de VLANs permitidas y lista de VLANs activas.

```
SW1#show interfaces trunk

Port     Mode           Encapsulation  Status        Native vlan
Gi0/1    desirable      802.1q         trunking      1

Port     Vlans allowed on trunk
Gi0/1    1-2,4-4094

Port     Vlans allowed and active in management domain
Gi0/1    1,4

Port     Vlans in spanning tree forwarding state and not pruned
Gi0/1    1,4
```

La ausencia de una VLAN en la última parte de la salida del comando no necesariamente significa que haya ocurrido un problema. De hecho, una VLAN podría estar legítimamente excluida de un troncal por cualquiera de las razones esgrimidas justo antes del Ejemplo 3.6. Sin embargo, para una pregunta de examen dada, puede ser útil conocer por qué el tráfico de una VLAN no será enviado por un troncal. En la salida del comando show interfaces trunk las tres listas de VLANs muestran una progresión de razones de por qué una VLAN no está enviando por un troncal. Para recordar los detalles, repase los detalles relativos al Ejemplo 1.4 del Capítulo 1 y unos pocos párrafos antes del ejemplo.

También en este paso se debe verificar la configuración VLAN nativa del troncal. El ID VLAN nativo puede establecerse manualmente para diferentes VLANs en cualquier extremo del troncal. Si las VLANs nativas son diferentes, los switches causarán accidentalmente que las tramas dejen una VLAN y entren en otra. Por ejemplo, si el switch SW1 envía una trama utilizado la VLAN nativa 1 en un troncal 802.1Q, SW1 no añade una cabecera VLAN, como es normal para la VLAN nativa. Cuando el switch SW2 recibe la trama, dándose cuenta de que no existe una cabecera 802.1Q, SW2 asume que la trama es parte de la VLAN nativa configurada de SW2. Si SW2 ha sido configurado para pensar que la VLAN 2 es la VLAN nativa en ese troncal, SW2 tratará de enviar la trama recibida en la VLAN 2.

La segunda clase general de problemas de *trunking* es que una interfaz que debe formar un troncal no lo haga. La causa más probable de este problema es una mala configuración del *trunking* en los extremos opuestos del enlace. El subcomando de interfaz `switchport mode {access | trunk | dynamic {desirable | auto}}` le dice a la interfaz si es troncal y las reglas con las que negociar el *trunking*. Se puede mostrar cualquier modo de *trunking* administrativo (configurado) de interfaz, así como el establecido por este comando de configuración, utilizando el comando `show interface switchport`. Asegúrese de que conoce el significado de cada una de las opciones de este comando de configuración (consulte la Tabla 1.4 del Capítulo 1), y las combinaciones en el otro extremo del segmento que resultan en el *trunking*, como se especificaron en la Tabla 1.5 del Capítulo 1.

En algunos casos, una interfaz puede fallar al utilizar el *trunking* por una falta de configuración del tipo de *trunking* (con otras palabras, si utilizar ISL u 802.1Q). Por ejemplo, si dos switches en los extremos opuestos de un segmento se configuran con los comandos `switchport trunk encapsulation isl` y `switchport trunk encapsulation dot1Q`, respectivamente, el troncal no podrá formarse, porque el tipo de troncal (la encapsulación) no coincide.

Ejemplo: resolución de problemas del plano de datos

Esta sección muestra un ejemplo de cómo aplicar los pasos a una red y escenario particulares. El escenario incluye varios problemas basados en la Figura 3.5. Al comienzo, PC1, PC2 y PC3 no pueden hace ping a su gateway predeterminado, R1, con la dirección IP 2.2.2.9. Esta sección muestra cómo aplicar los procesos de resolución de problemas tratados a lo largo de este capítulo para descubrir los problemas y solucionarlos. Para referenciarlos más fácilmente, los pasos se han resumido aquí como sigue:

Paso 1 Verificar la exactitud y completar la información listada en el diagrama de red utilizando CDP.

Paso 2 Verificar problemas de interfaz de este modo:

a. Determinar el(los) código(s) de estado de la interfaz para cada interfaz requerida, y si no está en un estado conectado (*connect*) o *up*/*up*, resolver los problemas hasta que la interfaz alcance el estado conectado o *up*/*up*.

b. Para cada interfaz en un estado conectado (*up*/*up*), verificar también otros dos problemas: desigualdad de dúplex y alguna variación de seguridad de puerto desechando tramas a propósito.

Paso 3 Verificar los problemas de seguridad de puerto como sigue:

a. Identificar todas las interfaces en las que la seguridad de puerto está habilitada (show running-config o show port-security).

b. Determinar si está ocurriendo una violación de seguridad basándose en la parte de *modo-violación* de la configuración de seguridad de puerto de la interfaz, como sigue:

— shutdown: la interfaz estará en un estado *err-disabled*.

— restrict: la interfaz estará en un estado conectado, pero el comando show port-security interface mostrará un incremento en el contador de violaciones.

— protect: la interfaz estará en un estado conectado, y el comando show port-security interface no mostrará un incremento en el contador de violaciones.

c. En todos los casos, comparar la configuración de la seguridad de puerto con el diagrama así como con el campo "last source address" de la salida del comando show port-security interface.

Paso 4 Verificar las VLANs y los troncales VLAN como sigue:

a. Identificar todas las interfaces de acceso y sus VLANs de acceso asignadas, y reasignar en las VLANs correctas si es necesario.

b. Determinar si las VLANs existen (configuradas o aprendidas con VTP) y están activas en cada switch. Si no, configurar y activar las VLANs para resolver los problemas como sea necesario.

c. Identificar las interfaces de *trunking* operativas en cada switch, y determinar las VLANs que pueden enviar por cada troncal.

Paso 1: verificar la exactitud del diagrama utilizando CDP

El Ejemplo 3.7 muestra una variedad de ejemplos de salida de los comandos show cdp neighbors y show cdp entry en los tres switches de la Figura 3.5. Una sencilla comparación confirma los nombres y las interfaces de la figura, con la excepción de que la interfaz Fa0/9 de SW2 conecta con el router R1, en vez de la interfaz Fa0/10 de SW2 mostrada en la Figura 3.5.

Este error de documentación en la Figura 3.5 (especificando la interfaz Fa0/10 de SW2 en lugar de Fa0/9) no afecta al funcionamiento actual de la red. Sin embargo, se requería el *trunking* entre SW2 y R1, en la interfaz Fa0/9 de SW2 (no Fa0/10), que tendría que haber sido explícitamente configurada para habilitar el *trunking*, porque los routers no pueden negociar automáticamente el uso del *trunking*. El Capítulo 4 trata los detalles de la configuración del *trunking* en los routers.

Ejemplo 3.7. Verificación de la Figura 3.5 utilizando CDP.

```
SW1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID      Local Intrfce     Holdtme    Capability    Platform       Port ID
SW2            Gig 0/1           122        S I           WS-C2960-2     Gig 0/2
SW3            Gig 0/2           144        S I           WS-C3550-2     Gig 0/1
```

```
! Los próximos comandos en SW2
SW2#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID      Local Intrfce     Holdtme    Capability    Platform       Port ID
SW1            Gig 0/2           125        S I           WS-C2960-2     Gig 0/1
SW3            Gig 0/1           170        S I           WS-C3550-2     Gig 0/2
R1             Fas 0/9           157        R S I         1841           Fas 0/1
SW2#show cdp entry R1
-------------------------
Device ID: R1
Entry address(es):
  IP address: 2.2.2.10
Platform: Cisco 1841, Capabilities: Router Switch IGMP
Interface: FastEthernet0/9, Port ID (outgoing port): FastEthernet0/1
Holdtime : 150 sec

Version :
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(9)T,
RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright 1986-2006 by Cisco Systems, Inc.
Compiled Fri 16-Jun-06 21:26 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''
Duplex: full
Management address(es):
```

```
! Los próximos comandos en SW3
SW3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID      Local Intrfce     Holdtme    Capability    Platform       Port ID
SW1            Gig 0/1           154        S I           WS-C2960-2     Gig 0/2
SW2            Gig 0/2           178        S I           WS-C2960-2     Gig 0/1
```

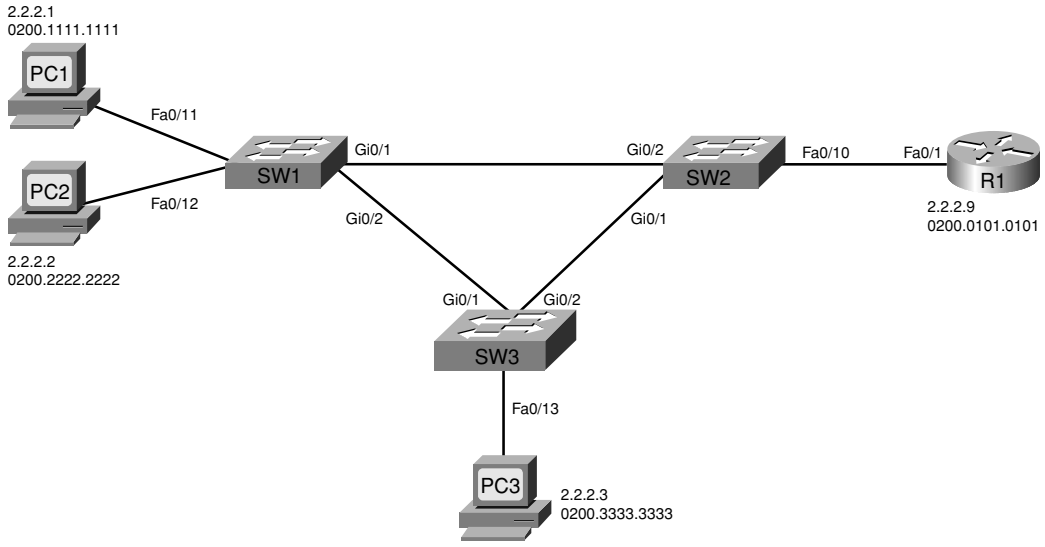


Figura 3.5. Ejemplo de red utilizada en la resolución de problemas del plano de datos.

Observe que CDP no identifica los problemas de documentación con las interfaces que conectan los PCs de usuario final; para los propósitos de este ejemplo, sepa que el resto de las interfaces mostradas en la Figura 3.5 son las interfaces correctas.

Paso 2: buscar problemas de interfaz

El siguiente paso examina el estado de la interfaz en cada una de las interfaces que deben estar actualmente en uso. El Ejemplo 3.8 lista varios comando show interface status en SW1 y SW3. (Para los propósitos de este capítulo, se asume que todas las interfaces de SW2 están funcionando correctamente.) Examine la salida, identifique cualquier problema que vea, y elabore una lista de otros problemas relativos a la interfaz que podría querer investigar más adelante basándose en esta salida.

Ejemplo 3.8. Problemas de interfaz en SW1.

```
SW1#show interfaces fa0/11 status

Port     Name      Status      Vlan        Duplex   Speed    Type
Fa0/11             connected   3           a-full   a-100    10/100BaseTX
SW1#show interfaces fa0/12 status

Port     Name      Status      Vlan        Duplex   Speed    Type
Fa0/12             notconnect  3           auto     auto     10/100BaseTX
SW1#show interfaces Gi0/1 status
```

(continúa)

Ejemplo 3.8. Problemas de interfaz en SW1 *(continuación)*.

```
Port      Name      Status       Vlan         Duplex   Speed    Type
Gi0/1               connected    trunk        a-full   a-1000   10/100/1000BaseTX
SW1#show interfaces Gi0/2 status

Port      Name      Status       Vlan         Duplex   Speed    Type
Gi0/2               connected    1            a-full   a-1000   10/100/1000BaseTX
```

```
! Cambiando a SW3
SW3#sh interfaces fa0/13 status

Port      Name      Status       Vlan         Duplex   Speed    Type
Fa0/13              connected    3            a-half   a-100    10/100BaseTX
SW3#show interfaces Gi0/1 status

Port      Name      Status       Vlan         Duplex   Speed    Type
Gi0/1               connected    1            a-full   a-1000   1000BaseTX
SW3#show interfaces Gi0/2 status

Port      Name      Status       Vlan         Duplex   Speed    Type
Gi0/2               connected    trunk        a-full   a-1000   1000BaseTX
```

Existe un problema obvio en SW1, con la interfaz Fa0/12 en estado de no conexión. Existen varias razones para que este estado exista, casi todas relacionadas con algún problema de cableado: desde que un cable no está completamente insertado en el puerto del switch hasta problemas de interferencia en el cable difíciles de encontrar. (Consulte la Tabla 3.2 para conocer las razones sugeridas.)

Las interfaces de SW3 parecen no tener problemas. Sin embargo, las tres interfaces tienen un valor dúplex que es el mismo valor que el switch podría utilizar si el proceso de autonegociación falla, con el uso de semidúplex en Fa0/3 como hecho destacable. Esto abre la posibilidad de que se produzca uno de los dos problemas de interfaces ya mencionados en este capítulo cuando la interfaz está en un estado conectado, llamado, desigualdad de dúplex.

Se puede determinar que las interfaces Gigabit 0/1 y 0/2 de SW3 no tienen una desigualdad simplemente utilizando el comando de estado show interfaces en el otro extremo de estos enlaces, SW1 y SW2 respectivamente. Sin embargo, los puertos conectados a un PC plantean el problema de que probablemente no podrá estar cerca del PC, así que podría tener que guiar al usuario final a través de los pasos para verificar los valores de velocidad y dúplex. Sin embargo, es útil observar los signos reveladores de *runts*, colisiones y colisiones recientes, como se lista en la salida del comando show interfaces en el Ejemplo 3.9.

En este caso, existe de hecho una desigualdad de dúplex. Sin embargo, tenga en cuenta que estos mismos contadores se incrementan bajo condiciones normales de operación semidúplex; por tanto, estos contadores no identifican definitivamente el problema como una desigualdad de dúplex.

Ejemplo 3.9. Signos de una desigualdad de dúplex.

```
SW3#show interfaces fa0/13
FastEthernet0/13 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 000a.b7dc.b78d (bia 000a.b7dc.b78d)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     108 packets input, 6946 bytes, 0 no buffer
     Received 3 broadcasts (0 multicast)
     54 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 2 multicast, 0 pause input
     0 input packets with dribble condition detected
     722 packets output, 52690 bytes, 0 underruns
     0 output errors, 114 collisions, 5 interface resets
     0 babbles, 78 late collision, 19 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

En este caso, la configuración de SW3 fue cambiada para utilizar full-dúplex en la interfaz Fa0/13, para ser igual a la configuración manual en PC3.

Paso 3: buscar problemas de seguridad de puerto

El siguiente paso examina la configuración y el estado de la seguridad de puerto en cada switch. Comenzar con el comando show port-security es particularmente útil porque lista las interfaces en las cuales la característica ha sido habilitada. El Ejemplo 3.10 muestra estos comandos en SW1 y SW2, además de algunos otros pocos comandos. Observe que SW2 y SW3 no tienen la característica de seguridad de puerto habilitada.

Examine la salida del Ejemplo 3.10, y antes de leer más allá del final del ejemplo, haga unas pequeñas notas acerca de cuáles deberían ser los siguientes pasos para eliminar la seguridad de puerto como un problema potencial, o bien qué comando debería utilizar para aislar un problema potencial.

Ejemplo 3.10. Seguridad de puerto en SW1 y SW2.

```
SW1#show port-security
Secure Port    MaxSecureAddr  CurrentAddr    SecurityViolation   Security Action
                 (Count)        (Count)           (Count)
-------------------------------------------------------------------------------
    Fa0/11               1            1                  97          Restrict
-------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)       : 0
Max Addresses limit in System (excluding one mac per port)   : 8320
```

```
! En SW2, no hay interfaces con la seguridad de puerto habilitada.
SW2#show port-security
Secure Port    MaxSecureAddr  CurrentAddr    SecurityViolation   Security Action
                 (Count)        (Count)           (Count)
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)       : 0
Max Addresses limit in System (excluding one mac per port)   : 8320
```

Los comandos show port-security en este ejemplo muestran las interfaces en las cuales se ha habilitado la seguridad de puerto: concretamente, la interfaz Fa0/11 de SW1 y ninguna interfaz en SW2. En SW1, los elementos destacables para la resolución de problemas son las denominadas acciones de seguridad (Security Action), que coinciden con los valores establecidos en el modo de violación, y muestran una acción de restringido (*restrict*). Con la configuración de restricción, la interfaz Fa0/11 de SW1 puede estar en estado conectado (*connect*) (como se ve en el Ejemplo 3.8), pero la seguridad de puerto puede descartar tráfico que viole la configuración de seguridad de puerto. Por tanto, es necesario un examen más detallado de la configuración de la seguridad de puerto, como se muestra en el Ejemplo 3.11.

Ejemplo 3.11. Seguridad de puerto en SW1 y SW2.

```
SW1#show port-security interface fa0/11
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode               : Restrict
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 1
Total MAC Addresses          : 1
Configured MAC Addresses     : 1
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : 0200.1111.1111:3
Security Violation Count     : 97
!
```

(continúa)

Ejemplo 3.11. Seguridad de puerto en SW1 y SW2 *(continuación).*

```
! A continuación, la configuración muestra que la dirección MAC configurada no es
! igual a la dirección MAC de PC1
SW1#show running-config interface fa0/11

interface FastEthernet0/11
 switchport access vlan 3
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.3333.3333
!
! El siguiente mensaje de registro también apunta a un problema de seguridad
! de puerto
01:46:58: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused
by MAC address 0200.1111.1111 on port FastEthernet0/11.
```

El ejemplo comienza confirmando el modo de seguridad y el contador de violaciones, así como mostrando la última dirección MAC (0200.1111.1111) en enviar una trama por la interfaz Fa0/11. La dirección MAC de PC1 (0200.1111.1111) no coincide con la configuración de seguridad de puerto como puede verse en la segunda parte del ejemplo, una configuración que tiene como valor predefinido un máximo de una dirección MAC con una dirección MAC explícitamente configurada de 0200.3333.3333. Una sencilla solución es reconfigurar la seguridad de puerto para que muestre la dirección MAC de PC1. Observe que el ingeniero podría necesitar usar los comandos shutdown y después no shutdown en esta interfaz para recuperarla, ya que la configuración utiliza el modo de violación restringido (*restrict*), el cual deja la interfaz *up* mientras descarte tráfico hacia/desde PC1.

Finalmente, el final del ejemplo muestra un mensaje de registro generado para cada violación cuando se utiliza el modo restringido (*restrict*). Este mensaje podría ser visto en consola o con una conexión Telnet o Shell seguro (SSH) al switch, si el usuario remoto ha ejecutado el comando EXEC terminal monitor.

Paso 4: buscar problemas de VLAN y de troncales VLAN

El Paso 4A comienza examinando las interfaces de acceso para garantizar que las interfaces han sido asignadas a las VLANs correctas. En este caso, todas las interfaces conectadas a los PCs y los routers de la Figura 3.5 deben estar asignados a la VLAN 3. El Ejemplo 3.12 proporciona algunos resultados útiles del comando show. Tómese un momento para leer el ejemplo, y busque cualquier problema de asignación de VLAN.

El único problema en este caso es el hecho de que mientras la interfaz Fa0/10 de SW2 se asignó a la VLAN 3, según el dibujo de la Figura 3.5, SW2 conecta con R1 utilizando Fa0/9 (como veíamos con CDP en el Ejemplo 3.7). La interfaz Fa0/9 está de forma predeterminada en la VLAN 1. Para solucionar este problema particular, en SW2, configurar el subcomando de interfaz switchport access vlan 3 en la interfaz Fa0/9.

Ejemplo 3.12. Verificando las asignaciones de VLAN a la interfaz de acceso.

```
SW1#show interfaces fa0/11 status
Port      Name        Status        Vlan        Duplex  Speed   Type
Fa0/11                connected     3           a-full  a-100   10/100BaseTX
SW1#show interfaces fa0/12 status

Port      Name        Status        Vlan        Duplex  Speed   Type
Fa0/12                notconnect    3           auto    auto    10/100BaseTX
```

```
! En SW2
SW2#show interfaces status
! líneas omitidas por brevedad
Fa0/9                 connected     1           a-full  a-100   10/100BaseTX
Fa0/10                notconnect    3           auto    auto    10/100BaseTX
```

```
! En SW3
SW3#show interfaces fa0/13 status

Port      Name        Status        Vlan        Duplex  Speed   Type
Fa0/13                connected     3           full    a-100   10/100BaseTX
```

La siguiente parte del Paso 4 (Paso 4B) sugiere validar las VLANs para asegurar que las VLANs están activas en cada switch. El ejemplo en curso sólo utiliza la VLAN 3, así el Ejemplo 3.13 muestra que la VLAN 3 es conocida de hecho en cada switch. Cuando lea el ejemplo, busque cualquier problema con VLAN 3.

Ejemplo 3.13. Encontrando un problema de semidúplex.

```
SW1#show vlan id 3

VLAN  Name                             Status    Ports
----  -------------------------------- --------- -------------------------------
3     book-vlan3                       active    Fa0/11, Fa0/12, Gi0/1, Gi0/2
! líneas omitidas por brevedad
```

```
! En SW2
SW2#show vlan brief

VLAN  Name                             Status    Ports
----  -------------------------------- --------- -------------------------------
1     default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
3     VLAN0003                         active    Fa0/9, Fa0/10
! líneas omitidas por brevedad
```

(continúa)

Ejemplo 3.13. Encontrando un problema de semidúplex *(continuación).*

```
! En SW3
SW3#show vlan brief

VLAN   Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1      default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                  Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                  Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                  Fa0/22, Fa0/23, Fa0/24
3      book-vlan3 active Fa0/13
! Se han omitido líneas para abreviar
```

En este caso, la VLAN 3 existe y está activa en los tres switches. Sin embargo, SW2 muestra un nombre diferente al de los otros dos switches. El nombre no es importante para el funcionamiento de la VLAN; por tanto, esta diferencia no importa. Como resultado, SW2 está utilizando VTP en modo transparente, con SW1 y SW3 en modo cliente y servidor VTP, respectivamente. Y el nombre de VLAN 3 (book-vlan3) coincide en SW1 y SW3.

Finalmente, la última parte del Paso 4 de la resolución de problemas (Paso 4C) sugiere confirmar el estado del *trunking* de todas las interfaces troncales esperadas. Es también útil determinar en cada troncal las VLANs que enviará. El Ejemplo 3.14 muestra salidas que ayudan a encontrar las respuestas. Examine la salida del ejemplo, y antes de leer más allá del final del mismo, liste cualquier troncal que no envíe tráfico actualmente en VLAN 3, y haga una lista de las posibles razones de por qué VLAN 3 es omitida en el troncal.

Ejemplo 3.14. Verificación del *trunking* y de VLAN 3.

```
SW1#show interfaces trunk

Port        Mode             Encapsulation      Status         Native vlan
Gi0/1       desirable        802.1q             trunking       1
Gi0/2       desirable        802.1q             trunking       1

Port        Vlans allowed on trunk
Gi0/1       1-4094
Gi0/2       1-4094

Port        Vlans allowed and active in management domain
Gi0/1       1,3
Gi0/2       1,3
```

(continúa)

Ejemplo 3.14. Verificación del *trunking* y de VLAN 3 *(continuación).*

```
SPort   Vlans in spanning tree forwarding state and not pruned
Gi0/1       3
Gi0/2       1,3
```

```
! A continuación, SW2
SW2#show interfaces trunk

Port        Mode            Encapsulation     Status         Native vlan
Gi0/1       auto            802.1q            trunking       1
Gi0/2       auto            802.1q            trunking       1

Port        Vlans allowed on trunk
Gi0/1       1-4094
Gi0/2       1-4094

Port        Vlans allowed and active in management domain
Gi0/1       1,3
Gi0/2       1,3

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       1,3
Gi0/2       1
```

```
! A continuación, SW3
SW3#show interfaces trunk

Port        Mode            Encapsulation     Status         Native vlan
Gi0/1       auto            n-802.1q          trunking       1
Gi0/2       desirable       n-802.1q          trunking       1

Port        Vlans allowed on trunk
Gi0/1       1-4094
Gi0/2       1-4094

Port        Vlans allowed and active in management domain
Gi0/1       1,3
Gi0/2       1,3

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       1,3
Gi0/2       1,3!
```

Examinando el final del comando show interfaces trunk en cada switch, se puede ver que de ambas interfaces en cada switch, sólo la interfaz Gi0/2 de SW2 no está enviando tráfico actualmente de la VLAN 3. Anteriormente en este capítulo, en la sección "Identificar los troncales y las VLANs enviadas en esos troncales", se especificaron cuatro razones por las que una VLAN podría ser excluida de un troncal. Sin embargo, tres de estas cuatro razones pueden ser descartadas basándose en la salida de los comandos del Ejemplo 3.14

y en unos pocos ejemplos de este capítulo. Primero, si VLAN 3 fue excluida porque no está en la lista de VLANs permitidas, o porque VLAN 3 no está activa, la VLAN 3 no se omitiría de las primeras dos listas de VLANs del comando show interfaces trunk en SW2. También, el *pruning* VTP puede descartarse porque los ejemplos anteriores mostraban que los tres switches tienen al menos una interfaz en VLAN 3 y en un estado conectado, por lo que si los tres switches utilizan VTP correctamente, con el *pruning* VTP habilitado, VLAN 3 podría no ser recortada. Por tanto, VLAN 3 es omitida en este caso por STP.

Después de encontrar todos los problemas en el ejemplo en curso, y solucionarlos, PC1, PC3 y R1 pueden todos hacer ping entre ellos. PC2, con un problema de cableado sin especificar, todavía no funciona.

Predicción del funcionamiento normal del plano de datos de conmutación LAN

Uno de los pasos de la resolución de problemas es analizar qué debería estar pasando para poder comparar con lo que está pasando realmente, con la esperanza de aislar la causa raíz de cualquier problema. Estas últimas secciones del Capítulo 3 completa el examen que hace este capítulo de cómo las LANs deberían funcionar examinando dos ejemplos de tramas enviadas a través de una versión operativa del mismo ejemplo de red utilizado de ejemplo para la resolución de problemas que se acaba de completar. El objetivo es explicar cómo interpretar la salida actual del comando show en los switches para predecir por dónde enviarán una trama en particular. El primer ejemplo muestra una trama de difusión enviada por PC1 en la Figura 3.5, y el segundo muestra el proceso de envío de una trama de unidifusión enviada por R1 a la dirección MAC de PC1.

PC1 difunde en VLAN 1

El primer ejemplo operativo del plano de datos examina la ruta de una difusión enviada por PC1. PC1 podría no tener en su caché ARP la dirección MAC de R1, por lo que en este caso, PC1 envía una difusión ARP, con una dirección IP de destino de 255.255.255.255 y una dirección Ethernet de destino de FFFF.FFFF.FFFF. Esta sección examina que los distintos switches no envían la difusión a todas las partes de la VLAN 3, como se muestra en la Figura 3.6.

Para analizar el flujo de la difusión, observe el proceso genérico de envío, que se resume en la sección "Visión general del proceso de envío de conmutación LAN normal", anteriormente en este capítulo. Los ejemplos anteriores confirmaban que el puerto Fa0/11 de SW1 está asignado a la VLAN 3 y que la interfaz Fa0/11 de SW1 es una interfaz de acceso. Debido a que la trama es de difusión, SW1 inundará la trama. Conociendo estos hechos, el Ejemplo 3.15 lista información suficiente para predecir las interfaces de salida por las que SW1 enviará la trama de difusión enviada por PC1 gracias a la salida del comando show spanning-tree vlan 3 active.

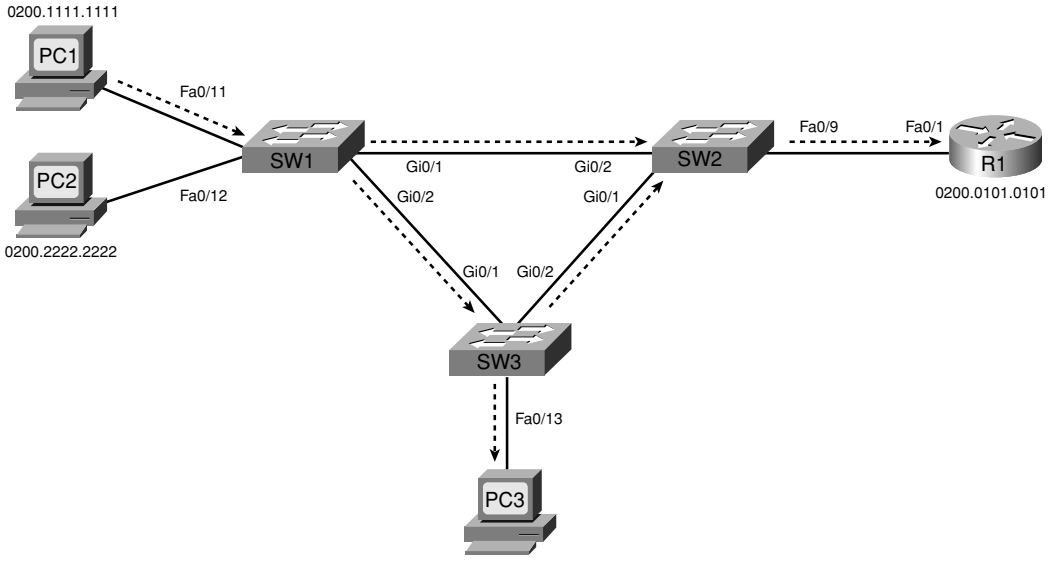


Figura 3.6. Ruta de envío entre PC1 y R1 para el Ejemplo 3.14.

Ejemplo 3.15. Lista de las interfaces activas en SW1.

```
SW1#show spanning-tree vlan 3 active

VLAN0003
  Spanning tree enabled protocol ieee
  Root ID     Priority    24579
              Address     000a.b7dc.b780
              Cost        1
              Port        26 (GigabitEthernet0/2)
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID   Priority    32771      (priority 32768 sys-id-ext 3)
              Address     0019.e86a.6f80
              Hello Time  2   sec Max Age 20 sec    Forward Delay 15 sec
              Aging Time  300

Interface      Role Sts Cost     Prio.Nbr      Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/11         Desg FWD          19 128.11     P2p
Gi0/1          Desg FWD          4 128.25      P2p
Gi0/2          Root FWD          1 128.26      P2p
```

Observe que SW1 no enviará la trama de vuelta por Fa0/11 ya que la trama llega por esta misma interfaz. Además, SW1 enviará la trama por las interfaces troncales (Gi0/1 y Gi0/2). También, anteriormente en este capítulo, el Ejemplo 3.14 mostraba evidencias de que los troncales de SW1 utilizan 802.1Q, con VLAN 1 nativa, por lo que SW1 añadirá

una cabecera 802.1Q, con el ID VLAN 3, a cada copia de la trama de difusión enviada por estos dos troncales.

Las acciones de SW1 significan que SW2 y SW3 deberían recibir una copia de la trama de difusión enviada por PC1. En el caso de SW2, SW2 pasa a descartar su copia de la trama de difusión recibida de PC1 por su interfaz Gi0/2. SW2 descarta la trama por el Paso 3 del proceso genérico de envío explicado anteriormente en este capítulo, porque la interfaz entrante (Gi0/2) de SW2 está en un estado de Bloqueo en VLAN 3. (El Ejemplo 3.14 y el texto que sigue a este ejemplo mostraban a la interfaz Gi0/2 de SW2 en un estado de Bloqueo para VLAN 3.) Observe que el estado de Bloqueo de SW2 no impide a SW1 enviar la trama a SW2; en cambio, SW2 descarta silenciosamente la trama recibida.

Para la copia de la trama de difusión de PC1 recibida por SW3 en su interfaz Gi0/1, SW3 inunda la trama. SW3 determina la VLAN de la trama basándose en la cabecera entrante 802.1Q y encuentra la interfaz entrante en un estado de Envío STP. Basándose en estos hechos, SW3 enviará la trama por la VLAN 3. El Ejemplo 3.16 muestra la información que es necesaria para conocer por qué interfaces SW3 envía la difusión VLAN 3.

Ejemplo 3.16. SW3: envío de una difusión en VLAN 3.

```
SW3#show mac address-table dynamic vlan 3
Mac Address Table
-------------------------------------------

Vlan    Mac Address        Type       Ports
-----   ------------       --------   -----
  3     0200.0101.0101     DYNAMIC    Gi0/2
  3     0200.1111.1111     DYNAMIC    Gi0/1
  3     0200.3333.3333     DYNAMIC    Fa0/13
Total Mac Addresses for this criterion: 3

SW3#show spanning-tree vlan 3 active

VLAN0003
  Spanning tree enabled protocol ieee
  Root ID     Priority     24579
              Address      000a.b7dc.b780
              This bridge is the root
              Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID   Priority     24579 (priority 24576 sys-id-ext 3)
              Address      000a.b7dc.b780
              Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts  Cost     Prio.Nbr   Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/13           Desg FWD  19       128.13     P2p
Gi0/1            Desg FWD  4        128.25     P2p
Gi0/2            Desg FWD  4        128.26     P2p
```

De igual forma que SW1, SW3 no enviará la difusión por la misma interfaz por la que llegó la trama (Gi0/1 en este caso), pero SW3 inunda la trama por todas sus otras interfaces de esa VLAN y en un estado de Envío STP, llamadas Fa0/13 y Gi0/2. Además, debido a que la interfaz Gi0/2 de SW3 utiliza el *trunking* 802.1Q, con VLAN 1 nativa, SW3 añade una cabecera 802.1Q con ID VLAN 3.

Finalmente, cuando SW2 recibe una copia de difusión por su interfaz Gi0/1 procedente de SW3, SW2 sigue el mismo proceso genérico que los otros switches. SW2 identifica la VLAN basándose en la cabecera 802.1Q entrante, confirma que la interfaz entrante está en estado de Envío, e inunda la difusión por todas sus interfaces en estado de Envío y en la VLAN 3. En este caso, SW2 envía la trama sólo por la interfaz Fa0/9, conectada al router R1. El Ejemplo 3.17 muestra la salida de los comandos que lo corroboran.

Ejemplo 3.17. SW2: envío de una difusión en la VLAN3 recibida de SW3.

```
! Primero, observe que la dirección de difusión FFFF.FFFF.FFFF no está
! en la tabla de direcciones MAC.
SW2#show mac address-table dynamic vlan 3
Mac Address Table
-------------------------------------------

Vlan    Mac Address        Type       Ports
-----   ------------       --------    -----
3       000a.b7dc.b79a     DYNAMIC    Gi0/1
3       0200.0101.0101     DYNAMIC    Fa0/9
3       0200.1111.1111     DYNAMIC    Gi0/1
3       0200.3333.3333     DYNAMIC    Gi0/1
Total Mac Addresses for this criterion: 4
! Después, observe que Fa0/9 y Gi0/1 están en estado de envío STP
! y la difusión llega por Gi0/1 – por lo que SW2 inunda la trama sólo por Fa0/9.
SW2#show spanning-tree vlan 3 active
!líneas omitidas por brevedad

Interface        Role Sts  Cost     Prio.Nbr  Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/9            Desg FWD  19       128.9     P2p
Gi0/1            Root FWD  4        128.25    P2p
Gi0/2            Altn BLK  4        128.26    P2p
```

SW2 no envía la trama por Gi0/1, porque la trama entra por la interfaz Gi0/1 de SW2.

Ruta de envío: unidifusión de R1 a PC1

El segundo ejemplo del plano de datos examina cómo los switches envían una trama de unidifusión. Para analizar el proceso de envío para tramas de unidifusión, considerar la res-

puesta ARP de R1 en respuesta a la solicitud/difusión ARP de PC1. Las direcciones de destino (ambas, IP y MAC) de la respuesta ARP de R1 son las direcciones IP y MAC de PC1, respectivamente. La Figura 3.7 muestra la ruta de envío, con los ejemplos que siguen explicando cómo se aplica en este caso particular el proceso general de envío.

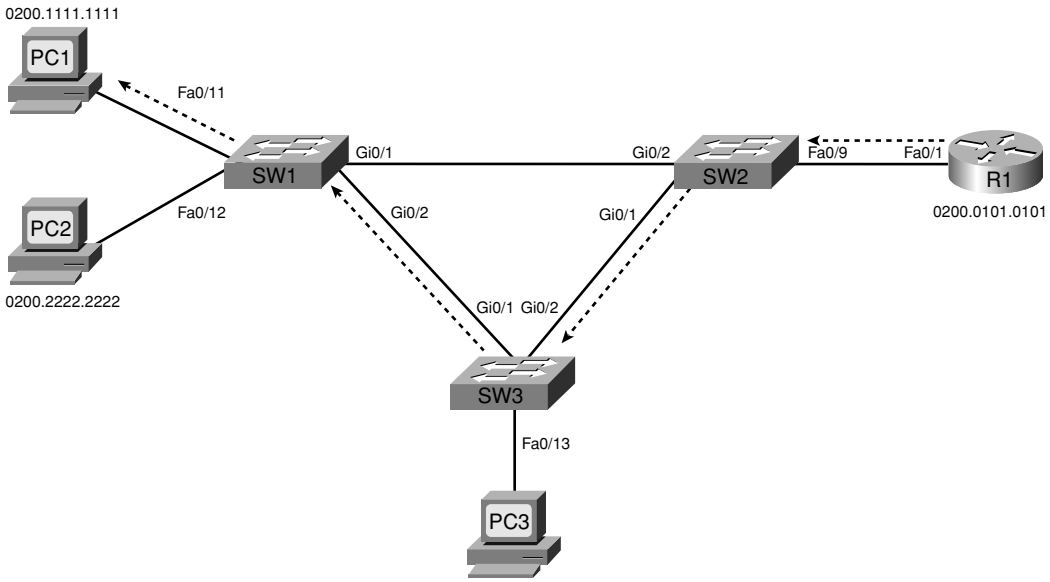


Figura 3.7. Ruta de envío desde R1 a PC1 para el Ejemplo 3.15.

Cuando SW2 recibe la trama de R1, SW1 observa que la trama entra por la interfaz Fa0/9, una interfaz de acceso en VLAN 3. El final del Ejemplo 3.17 mostraba a Fa0/9 en un estado de Envío en VLAN 3, por lo que SW2 intentará enviar la trama en lugar de descartarla. Como puede verse después en el Ejemplo 3.18, la tabla de direcciones MAC de SW2 lista la dirección MAC de PC1 (0200.1111.1111) de la interfaz Gi0/1 y en la VLAN 3; así, SW2 envía la trama por Gi0/1 a SW3.

Ejemplo 3.18. Lógica de SW2 cuando envía una unidifusión conocida a PC1.

```
SW2#show mac address-table dynamic vlan 3
Mac Address Table
-------------------------------------------

Vlan    Mac Address        Type       Ports
-----   ------------       --------    -----
3       000a.b7dc.b79a     DYNAMIC    Gi0/1
3       0200.0101.0101     DYNAMIC    Fa0/9
3       0200.1111.1111     DYNAMIC    Gi0/1
Total Mac Addresses for this criterion: 3
```

Cuando SW3 recibe la trama desde SW2, SW3 observa que la trama entra por la interfaz Gi0/2, una interfaz troncal, y que la cabecera de *trunking* contiene el ID VLAN 3. La parte final del Ejemplo 3.16 mostraba a Gi0/2 en un estado de Envío STP en la VLAN 3 (enviando Paso 3); por tanto, SW3 no podrá descartar la trama recibida debido a STP. Como se muestra después en el Ejemplo 3.19, la tabla de direcciones MAC de SW3 lista la dirección MAC de PC1 (0200.1111.1111) de la interfaz Gi0/1 y en la VLAN 3; por tanto, SW3 envía la trama por Gi0/1 a SW1.

Ejemplo 3.19. Lógica de SW3 cuando envía una unidifusión conocida a PC1.

```
SW3#show mac address-table dynamic vlan 3
Mac Address Table
-------------------------------------------

Vlan    Mac Address        Type       Ports
-----   ------------       --------   -----
  3     0200.0101.0101     DYNAMIC    Gi0/2
  3     0200.1111.1111     DYNAMIC    Gi0/1
  3     0200.3333.3333     DYNAMIC    Fa0/13
Total Mac Addresses for this criterion: 3
```

Cuando SW1 recibe la trama desde SW3, SW1 observa que la trama entra por la interfaz Gi0/2, una interfaz troncal, y que la cabecera de *trunking* contiene el ID VLAN 3. La parte final del Ejemplo 3.15 mostraba a Gi0/2 de SW1 en un estado de Envío STP en la VLAN 3; por tanto, SW1 no descartará la trama porque la interfaz no está en un estado de envío STP.

Como se ve después en el Ejemplo 3.20, la tabla de direcciones MAC de SW1 lista la dirección MAC de PC1 (0200.1111.1111) de la interfaz Fa0/11 y VLAN 3, por lo que SW1 enviará la trama por su interfaz Fa0/11 a PC1. En este caso, SW1 elimina la cabecera VLAN 802.1Q, porque la interfaz Fa0/11 es una interfaz de acceso.

Ejemplo 3.20. Lógica de SW1 cuando envía una unidifusión conocida a PC1.

```
SW1#show mac address-table dynamic vlan 3
Mac Address Table
-------------------------------------------

Vlan    Mac Address        Type       Ports
-----   ------------       --------   -----
  3     000a.b7dc.b799     DYNAMIC    Gi0/2
  3     0200.0101.0101     DYNAMIC    Gi0/2
  3     0200.3333.3333     DYNAMIC    Gi0/2
Total Mac Addresses for this criterion: 3
SW1#show mac address-table vlan 3
          Mac Address Table
-------------------------------------------
```

(continúa)

Ejemplo 3.20. Lógica de SW1 cuando envía una unidifusión conocida a PC1 *(continuación).*

```
Vlan     Mac Address         Type       Ports
-----    ------------        --------    -----
All      0100.0ccc.cccc      STATIC     CPU
All      0100.0ccc.cccd      STATIC     CPU
All      0180.c200.0000      STATIC     CPU
All      0180.c200.0001      STATIC     CPU
All      0180.c200.0002      STATIC     CPU
All      0180.c200.0003      STATIC     CPU
All      0180.c200.0004      STATIC     CPU
All      0180.c200.0005      STATIC     CPU
All      0180.c200.0006      STATIC     CPU
All      0180.c200.0007      STATIC     CPU
All      0180.c200.0008      STATIC     CPU
All      0180.c200.0009      STATIC     CPU
All      0180.c200.000a      STATIC     CPU
All      0180.c200.000b      STATIC     CPU
All      0180.c200.000c      STATIC     CPU
All      0180.c200.000d      STATIC     CPU
All      0180.c200.000e      STATIC     CPU
All      0180.c200.000f      STATIC     CPU
All      0180.c200.0010      STATIC     CPU
All      ffff.ffff.ffff      STATIC     CPU
  3      000a.b7dc.b799      DYNAMIC    Gi0/2
  3      0200.0101.0101      DYNAMIC    Gi0/2
  3      0200.1111.1111      STATIC     Fa0/11
Total Mac Addresses for this criterion: 23
```

Este último paso señala un hecho importante acerca de la tabla de direcciones MAC y de la seguridad de puerto. Observe que el comando `show mac address-table dynamic` en SW1 no lista la dirección MAC de PC1, 0200.1111.1111, por lo que se podría tender a pensar que SW1 inundará la trama porque es una trama con una dirección de unidifusión desconocida. Sin embargo, debido a que SW1 ha configurado la seguridad de puerto en Fa0/11, incluyendo el subcomando de interfaz `switchport port-security mac-address 0200.1111.1111`, el IOS considera a esta dirección MAC como una dirección MAC estática. Por tanto, si se elimina la palabra clave `dynamic`, el comando `show mac address-table vlan 3` lista todas las direcciones MAC conocidas en la VLAN, incluida 0200.1111.1111. Esta salida del comando confirma que SW1 enviará la unidifusión a 0200.1111.1111 sólo por la interfaz Fa0/11.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 3.6 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 3.6. Temas clave del Capítulo 3.

Tema Clave	Descripción	Número de página
Tabla 3.2	Muestra el conjunto de códigos de estado de interfaz y las causas raíz de cada estado.	123
Figura 3.4	Usos típicos de los cables Ethernet recto y cruzado.	124
Tabla 3.3	Lista los dispositivos y los pines por los cuales transmiten en 10BASE-T y 100BASE-Tx.	124
Lista	Sugerencias para detectar un problema de desigualdad de dúplex.	127
Lista	Valor predeterminado de dúplex en la autonegociación IEEE elegido en función de la velocidad actual.	128
Lista	Características de la seguridad de puerto.	128
Tabla 3.4	Modos de violación de la seguridad de puerto con las diferencias de comportamiento y comandos show.	129
Tabla 3.5	Lista los comandos show útiles para encontrar las interfaces de acceso y sus VLANs asignadas.	133
Lista	Las cuatro razones por las que un switch no permite tráfico de una VLAN por un troncal particular.	135
Lista	Lista de los pasos de resolución de problemas explicados en este capítulo (no es necesario memorizarlos).	136-137

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD) o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas ya completas para validar su trabajo.

Temas* del examen ICND2 publicados por Cisco que se tratan en esta parte

Configuración, verificación y resolución de problemas en un switch con VLANs y comunicación entre switches

- Configuración, verificación y resolución de problemas de enrutamiento VLAN.

Implementación de un esquema de direccionamiento IP y de servicios IP para satisfacer los requisitos de red de la sede de una empresa de tamaño medio

- Calcular y aplicar un diseño de direccionamiento IP VLSM para una red.
- Determinar el esquema de direccionamiento sin clase apropiado utilizando VLSM y elaborar un resumen de cómo satisfacer los requisitos de direccionamiento en un entorno LAN/WAN.
- Identificar y corregir problemas comunes asociados con el direccionamiento IP y las configuraciones de host.

Configuración y resolución de problemas para el funcionamiento básico y el enrutamiento en dispositivos Cisco

- Verificar la configuración y conectividad utilizando ping, traceroute y telnet o SSH.
- Resolver problemas de implementación de enrutamiento.
- Verificar el funcionamiento del hardware y el software empleando comandos show y debug.
- Implementar la seguridad básica en los routers.

Implementar, verificar y resolver problemas con NAT y las ACLs en la red de la sede de una empresa de tamaño medio

- Describir el propósito y los tipos de listas de control de acceso.
- Configurar y aplicar listas de control de acceso basándose en unos requisitos de filtrado de red.
- Configurar y aplicar una lista de control de acceso que limite el acceso telnet y SSH a un router.
- Verificar y monitorizar las ACLs en un entorno de red.
- Resolver los problemas de implementación de las ACLs.

* No olvide consultar en http://www.cisco.com los últimos temas de examen publicados.

PARTE II

Enrutamiento IP

Capítulo 4 Enrutamiento IP: rutas estáticas y conectadas

Capítulo 5 VLSM y resumen de rutas

Capítulo 6 Listas de control de acceso IP

Capítulo 7 Resolución de problemas de enrutamiento IP

Este capítulo trata los siguientes temas:

Enrutamiento y direccionamiento IP: Esta sección revisa la relación entre el direccionamiento y el enrutamiento IP, y examina con más detalle cómo funciona el enrutamiento con múltiples rutas solapadas.

Rutas a subredes conectadas directamente: Esta sección examina cómo los routers añaden rutas para subredes conectadas a las interfaces del router.

Rutas estáticas: Esta sección describe cómo configurar rutas estáticas, incluyendo las rutas estáticas predeterminadas.

CAPÍTULO 4

Enrutamiento IP: rutas estáticas y conectadas

Este capítulo comienza la Segunda parte, "Enrutamiento IP". Los cuatro capítulos de esta parte se centran en las características que influyen en el proceso de enrutamiento (también llamado envío IP) con el cuál las computadoras y los routers envían paquetes desde la computadora de origen a la computadora de destino. Estos cuatro capítulos también explican ocasionalmente temas relacionados con los protocolos de enrutamiento IP, en parte porque el enrutamiento IP, una característica del plano de datos, confía fuertemente en el trabajo que en el plano de control hacen los protocolos de enrutamiento.

Este capítulo trata varios temas relativos a las rutas conectadas, que son las rutas que alcanzan subredes conectadas a una interfaz del router. Este capítulo también explica las rutas estáticas, incluyendo las rutas predeterminadas, así como los temas básicos interdependientes del direccionamiento IP y el enrutamiento IP.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las ocho preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 4.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

1. Un usuario de PC enciende su computadora, y tan pronto se inicia, abre en un navegador web la siguiente página: http://www.ciscopress.com. ¿Qué protocolo(s) podría definitivamente no ser utilizado por el PC durante este proceso?

a. DHCP

b. DNS

Tabla 4.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
Enrutamiento y direccionamiento IP	1-2
Rutas a subredes conectadas directamente	3-4
Rutas estáticas	5-8

c. ARP

d. ICMP

2. Un usuario de PC enciende su computadora, y tan pronto como se inicia, abre una ventana de comandos. Desde allí, ejecuta el comando ping 2.2.2.2, que muestra 100 por cien de éxito. La dirección IP del PC es 1.1.1.1 con la máscara 255.255.255.0. ¿Cuál de los siguientes valores podría ser necesario en el PC para soportar este exitoso ping?

a. La dirección IP de un servidor DNS.

b. La dirección IP de un gateway predeterminado.

c. La dirección IP de un servidor ARP.

d. La dirección IP de un servidor DHCP.

3. El Router 1 tiene una interfaz Fast Ethernet 0/0 con la dirección IP 10.1.1.1. La interfaz está conectada a un switch. Esta conexión se configura para migrar al *trunking* 802.1Q. ¿Cuál de los siguientes comandos podrían ser parte de una configuración válida de la interfaz Fa0/0 del Router 1?

a. interface fastethernet 0/0.4

b. dot1q enable

c. dot1q enable 4

d. trunking enable

e. trunking enable 4

f. encapsulation dot1q

4. Un router está configurado con el comando de configuración global no ip subnet-zero. ¿Cuál de los siguientes subcomandos de interfaz podría no ser aceptado por este router?

a. ip address 10.1.1.1 255.255.255.0

b. ip address 10.0.0.129 255.255.255.128

c. ip address 10.1.2.2 255.254.0.0

d. ip address 10.0.0.5 255.255.255.252

5. ¿Cuál de lo siguiente debe ser cierto antes de que el IOS liste una ruta como "S" en la salida de un comando show ip route?
   a. La dirección IP debe estar configurada en una interfaz.
   b. El router debe recibir una actualización de enrutamiento de un router vecino.
   c. El comando ip route debe ser añadido a la configuración.
   d. El comando ip address debe usar la palabra clave special.
   e. La interfaz debe estar *up* y *up*.
6. ¿Cuál de los siguientes comandos configura correctamente una ruta estática?
   a. ip route 10.1.3.0 255.255.255.0 10.1.130.253
   b. ip route 10.1.3.0 serial 0
   c. ip route 10.1.3.0 /24 10.1.130.253
   d. ip route 10.1.3.0 /24 serial 0
7. ¿Cuál de lo siguiente está afectado por si un router está realizando un enrutamiento con clase o sin clase?
   a. Cuándo usar una ruta predeterminada.
   b. Cuándo usar máscaras en las actualizaciones de enrutamiento.
   c. Cuándo convertir una dirección IP de destino del paquete en un número de red.
   d. Cuándo encolar basándose en la clasificación de un paquete en una cola particular.
8. Un router ha sido configurado con el comando de configuración global ip classless. El router recibe un paquete destinado a la dirección IP 168.13.4.1. El siguiente texto muestra el contenido de la tabla de enrutamiento del router. ¿Cuál de lo siguiente es verdadero acerca de cómo ese router envía el paquete?

```
Gateway of last resort is 168.13.1.101 to network 0.0.0.0

     168.13.0.0/24 is subnetted, 2 subnets
C       168.13.1.0 is directly connected, FastEthernet0/0
R       168.13.3.0 [120/1] via 168.13.100.3, 00:00:05, Serial0.1
```

   a. Es enviado a 168.13.100.3.
   b. Es enviado a 168.13.1.101.
   c. Es enviado por la interfaz Fa0/0, directamente a la computadora de destino.
   d. El router descarta el paquete.

Temas fundamentales

Este capítulo introduce varios conceptos directos acerca de cómo un router añade rutas a su tabla de rutas sin utilizar un protocolo de enrutamiento dinámico. En particular, este capítulo trata las rutas conectadas, incluyendo las rutas conectadas cuando un router uti-

liza el *trunking* LAN. También se tratan las rutas estáticas, con énfasis en cómo los routers utilizan rutas estáticas especiales llamadas rutas predeterminadas. Sin embargo, ya que este capítulo es el primero centrado en IP de este libro, comienza con una breve revisión de dos temas relacionados: enrutamiento y direccionamiento IP.

Nota

La introducción de este libro describe un plan alternativo de lectura para los lectores que preparan el examen CCNA 640-802, el cuál va de un lado a otro entre el libro *CCENT/CCNA ICND1 Guía oficial para el examen de certificación* y este libro. Si está usando ese plan, observe que la primera sección principal revisa los temas del libro ICND1. Si ha seguido este plan de lectura, puede avanzar a la sección "Envío IP por la ruta más específica".

Enrutamiento y direccionamiento IP

El enrutamiento IP depende de las reglas del direccionamiento IP, siendo uno de los objetivos de diseño original y principal del direccionamiento IP la creación de un enrutamiento IP eficiente. El enrutamiento IP define cómo un paquete IP puede ser entregado desde la computadora que crea el paquete hasta su destinatario. Las convenciones del direccionamiento IP agrupan las direcciones en conjuntos de direcciones consecutivas llamadas subredes que ayudan a los procesos de envío IP o enrutamiento IP.

Nota

Este libro utiliza los términos enrutamiento IP y envío IP como términos sinónimos. El término protocolos de enrutamiento IP se refiere a los protocolos de enrutamiento que los routers utilizan para llenar dinámicamente sus tablas de enrutamiento con las rutas actualmente mejores. Observe que algunos textos y cursos utilizan el término enrutamiento IP cuando se refieren a ambos, el proceso de envío de paquetes y los protocolos utilizados para aprender rutas.

Enrutamiento IP

Tanto las computadoras como los routers participan en el proceso de enrutamiento IP. La siguiente lista resume la lógica de una computadora cuando envía un paquete, asumiendo que la computadora está en una LAN Ethernet o una LAN inalámbrica:

Tema clave

1. Cuando se envía un paquete, comparar la dirección IP de destino del paquete con la percepción que tiene el host emisor del rango de direcciones de la subred conectada, basándose en la dirección IP del host y la máscara de subred.

a. Si el destino está en la misma subred que el host, enviar el paquete directamente al host de destino. Se necesita el Protocolo de resolución de direcciones (ARP, *Address Resolution Protocol*) para encontrar la dirección MAC del host de destino.

b. Si el destino no está en la misma subred que el host, enviar el paquete directamente al gateway predeterminado del host (router predeterminado). Se necesita ARP para encontrar la dirección MAC del gateway predeterminado.

Los routers utilizan los siguientes pasos generales, teniendo en cuenta que primero deben recibir el paquete, mientras que el host emisor (como se ha resumido previamente) comienza con el paquete IP en memoria:

1. Para cada trama recibida, utilizar el campo de secuencia de verificación de trama (FCS, *frame check sequence*) en la información final de enlace de datos para asegurar que la trama no contiene errores; si hay errores, descartar la trama (y no continuar con el siguiente paso).
2. Verificar la dirección de destino de capa de enlace de datos de la trama, y procesarla sólo si va dirigida a este router o a una dirección de difusión/multidifusión.
3. Descartar la cabecera y la información final de enlace de datos de la trama entrante, dejando el paquete IP.
4. Comparar la dirección IP de destino del paquete con la tabla de enrutamiento, y encontrar la ruta que coincida con la dirección de destino. Esta ruta identifica la interfaz saliente del router, y posiblemente el router de siguiente salto.
5. Determinar la dirección de enlace de datos de destino usada para enviar paquetes al siguiente router o computadora de destino (como indica la tabla de enrutamiento).
6. Encapsular el paquete IP en una nueva cabecera e información final de enlace de datos, apropiada para la interfaz saliente, y enviar la trama por esta interfaz.

Por ejemplo, considerar la Figura 4.1, que muestra una red sencilla con dos routers y tres computadoras. En este caso, PC1 crea un paquete para ser enviado a la dirección IP de PC3, 172.16.3.3. La figura muestra los tres pasos principales del enrutamiento, etiquetados como A, B y C: la lógica de enrutamiento de la computadora PC1 que envía el paquete a R1, la lógica de enrutamiento de R1 que envía el paquete a R2, y la lógica de enrutamiento de R2 que envía el paquete a PC2.

Primero se considera el Paso A de la Figura 4.1. PC1 muestra su propia dirección IP 172.16.1.1, máscara 255.255.255.0. (En este ejemplo todas las interfaces utilizan una máscara sencilla de subred, 255.255.255.0.) PC1 puede calcular su número de subred (172.16.1.0/24) y rango de direcciones (172.16.1.1–172.16.1.254). La dirección de destino 172.16.3.3 no está en la subred de PC1, de modo que PC1 usa el Paso 1B del resumen de la lógica de enrutamiento de host y envía el paquete, dentro de una trama Ethernet, a su gateway predeterminado con dirección IP 172.16.1.251.

El primer paso (Paso A) de PC1 enviando el paquete a su gateway predeterminado también revisa un par de conceptos importantes. Como puede verse en la parte inferior de la figura, PC1 utiliza su propia dirección MAC como la dirección MAC de origen, pero uti-

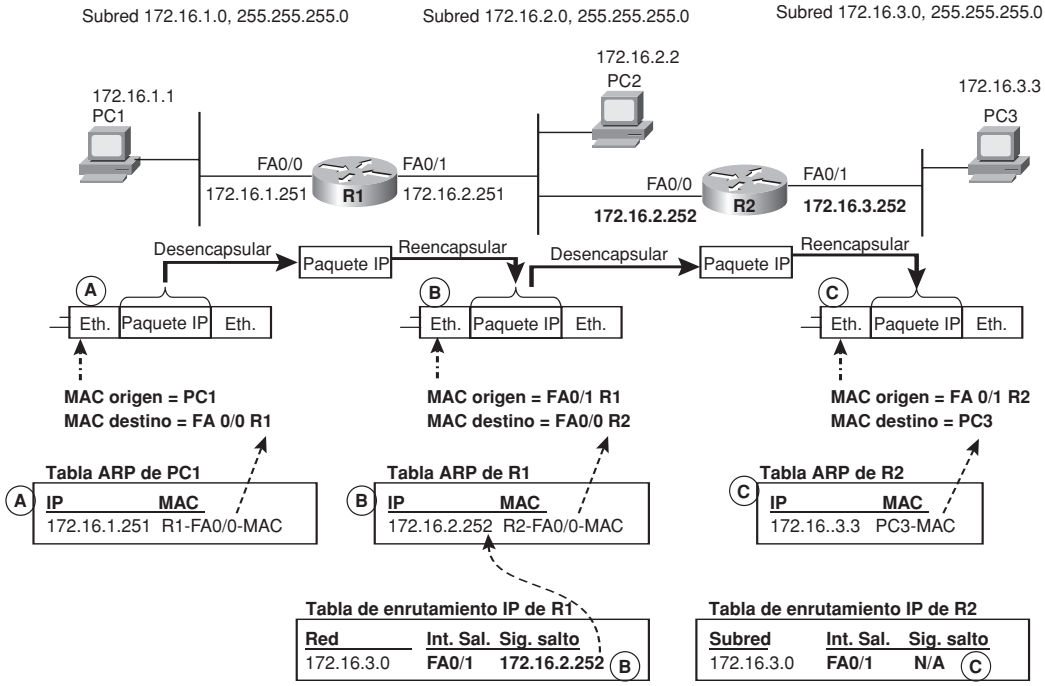


Figura 4.1. Ejemplo del proceso de enrutamiento IP.

liza la dirección MAC LAN de R1 como la dirección MAC de destino. Como resultado, cualquiera de los switches LAN puede entregar la trama correctamente a la interfaz Fa0/0 de R1. Observe también que PC1 busca y encuentra la dirección MAC de 172.16.1.251 en la caché ARP de PC1. Si la dirección MAC no se hubiera encontrado, PC1 podría haber tenido que usar ARP para descubrir dinámicamente la dirección MAC utilizada por 172.16.1.251 (R1) antes de poder enviar la trama como se muestra en la Figura 4.1.

Nos centramos ahora en el Paso B de la Figura 4.1, que es el trabajo realizado por el router R1 para enviar el paquete. Utilizando los seis pasos de enrutamiento resumidos que preceden a la Figura 4.1, en R1 ocurre lo siguiente. Observe que la figura denota muchos de los detalles con la letra *B*:

1. R1 verifica la FCS, y la trama no tiene errores.
2. R1 encuentra la dirección MAC de su interfaz Fa0/0 en el campo de dirección MAC de destino de la trama; por tanto, R1 debe procesar el paquete encapsulado.
3. R1 descarta la cabecera e información final de enlace de datos dejando el paquete IP (como se muestra directamente debajo del icono de R1 en la Figura 4.1).
4. (En la parte central inferior de la Figura 4.1) R1 compara la dirección IP de destino (172.16.3.3) con la tabla de enrutamiento de R1, encontrando la ruta coincidente mostrada en la figura, con la interfaz de salida Fa0/1 y el router 172.16.2.252 como siguiente salto.

5. R1 necesita encontrar la dirección MAC del dispositivo de siguiente salto (dirección MAC de R2), de modo que R1 busca y encuentra la dirección MAC en su tabla ARP.
6. R1 encapsula el paquete IP en una nueva trama Ethernet, con la dirección MAC de Fa0/1 de R1 como dirección MAC de origen, y la dirección MAC de Fa0/0 de R2 (por la tabla ARP) como la dirección MAC de destino. R1 envía la trama.

Aunque estos pasos pueden parecer laboriosos, piense en una versión más breve de esta lógica en los casos donde una pregunta no necesite este nivel de profundidad. Por ejemplo, en la resolución de problemas de enrutamiento, centrarse en el Paso 4 (la coincidencia de la dirección IP de destino del paquete con la tabla de enrutamiento del router) es probablemente uno de los pasos más importantes. Así, un breve resumen del proceso de enrutamiento podría ser el siguiente: el router recibe el paquete, busca la dirección de destino del paquete en la tabla de enrutamiento y envía el paquete como se indique en esa ruta. Aunque esta versión abreviada ignora algunos detalles, puede acelerar la resolución de problemas o las discusiones sobre temas de enrutamiento.

Para completar el ejemplo, considerar la misma lógica de envío de seis pasos de los routers aplicada en el router R2, etiquetada con la letra C en la Figura 4.1, como sigue:

1. R2 verifica la FCS, y la trama no tiene errores.
2. R2 encuentra su propia dirección MAC de la interfaz Fa0/0 en el campo de dirección MAC de destino de la trama; por esto, R2 procesa el paquete encapsulado.
3. R2 descarta la cabecera y la información final de enlace de datos, dejando el paquete IP (como se muestra directamente debajo del icono de R2 en la Figura 4.1).
4. (Parte inferior derecha de la Figura 4.1) R2 compara la dirección IP de destino (172.16.3.3) con la tabla de enrutamiento de R2, encontrando la ruta coincidente mostrada en la figura, con la interfaz Fa0/1 de salida y sin router de siguiente salto.
5. Ya que no existe router de siguiente salto, R2 necesita encontrar la dirección MAC del verdadero host de destino (dirección MAC de PC3); así, R2 busca y encuentra esta dirección MAC en su tabla ARP.
6. R2 encapsula el paquete IP en una nueva trama Ethernet, con la dirección MAC de Fa0/1 de R2 como la dirección MAC de origen, y la dirección MAC de PC3 (por la tabla ARP) como la dirección MAC de destino. R1 envía la trama.

Finalmente, cuando esta trama llega a PC3, PC3 ve su propia dirección MAC como dirección MAC de destino; por tanto, PC3 comienza a procesar la trama.

El mismo proceso general funciona también con enlaces WAN, con unos pocos detalles diferentes. En enlaces punto a punto, como los mostrados en la Figura 4.2, no se necesita una tabla ARP. Debido a que un enlace punto a punto debe tener al menos otro router conectado con él, el direccionamiento de enlace de datos se puede ignorar. Sin embargo, con Frame Relay, el proceso de enrutamiento sí considera las direcciones de enlace de datos, denominadas Identificadores de conexión de enlace de datos (DLCI). Los detalles de enrutamiento con respecto a los DLCIs de Frame Relay se tratan más adelante es este libro, en el Capítulo 13.

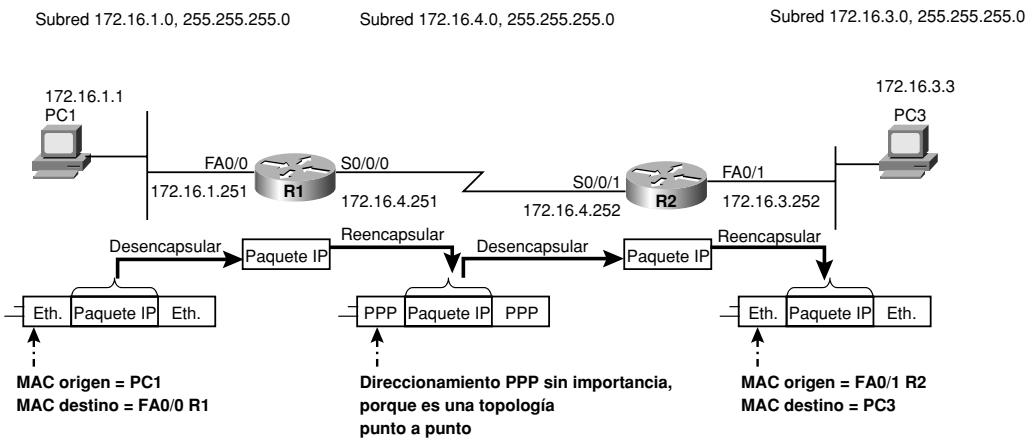


Figura 4.2. Ejemplo del proceso de enrutamiento IP.

El proceso de enrutamiento IP en los hosts y los routers confía en las habilidades de estos dispositivos para entender el direccionamiento IP y predecir qué direcciones IP están en cada grupo o subred. La siguiente sección proporciona una breve revisión de las direcciones y las subredes IP.

Direccionamiento y *subnetting* IP

Las reglas del direccionamiento IP ayudan a los procesos de enrutamiento IP organizando las direcciones IP en grupos de direcciones IP numeradas consecutivamente llamadas subredes. Para permitir una manera concisa de referirse a una subred, el direccionamiento IP define el concepto de un número y máscara de subred, que juntos identifican exactamente el rango de direcciones en una subred. Por ejemplo, los routers de las Figuras 4.1 y 4.2 utilizan rutas que listan el número de subred 172.16.3.0 cuando envían el paquete destinado a PC3 (172.16.3.3). Las figuras omiten la máscara de subred para reducir el desorden, pero cualquier dispositivo con el número de subred 172.16.3.0 y la máscara 255.255.255.0, sabe que estos dos números representan la siguiente subred:

- Número de subred 172.16.3.0
- Rango de direcciones utilizables en la subred: 172.16.3.1–172.16.3.254
- Dirección de difusión de la subred (no utilizable por hosts individuales): 172.16.3.255

La siguiente lista proporciona una breve revisión de algunos de los principales conceptos del direccionamiento IP. Observe que este capítulo solamente se refiere a direccionamiento IP versión 4 (IPv4); en el Capítulo 17, "IP Versión 6", se trata IPv6.

Tema clave

- Las direcciones IP de unidifusión son direcciones IP que pueden ser asignadas a una interfaz individual para enviar y recibir paquetes.
- Cada dirección IP de unidifusión pertenece a una red particular red de clase A, B o C, llamada red IP con clase.

- Si se usan subredes, lo que casi siempre es cierto en la vida real, cada dirección IP de unidifusión también pertenece a un subconjunto específico de red con clase llamado subred.
- La máscara de subred, escrita en cualquier formato, decimal con puntos (por ejemplo, 255.255.255.0) o notación de prefijo (por ejemplo, /24), identifica la estructura de las direcciones IP de unidifusión y permite a dispositivos y personas derivar el número de subred, el rango de direcciones y la dirección de difusión para una subred.
- Todos los dispositivos en la misma subred deben utilizar la misma máscara de subred; en caso contrario, los dispositivos tendrán opiniones diferentes acerca del rango de direcciones en la subred, lo que puede romper el proceso de enrutamiento IP.
- Los dispositivos en una única VLAN estarán en la misma única subred IP.
- Los dispositivos en diferentes VLANs estarán en diferentes subredes IP.
- Para enviar paquetes entre subredes, se debe usar un dispositivo que realice el enrutamiento. En este libro, sólo se muestran los routers, pero también se pueden usar los switches multicapa (los switches que también realizan funciones de enrutamiento).
- Los enlaces serie punto a punto usan diferente subred que las subredes LAN, pero estas subredes sólo necesitan dos direcciones IP, una para la interfaz de cada router en cada extremo del enlace.
- Los hosts separados por un router deben estar en subredes separadas.

La Figura 4.3 muestra un ejemplo entre redes que exhibe muchas de estas características. El switch SW1 de forma predeterminada pone todas sus interfaces en VLAN 1; por tanto, todos los hosts de la izquierda (incluido PC1) están en una única subred. Observe que la dirección IP de gestión de SW1, también en VLAN 1, será de esa misma subred. De forma similar, SW2 de forma predeterminada pone todos sus puertos en VLAN 1, necesitando una segunda subred. El enlace punto a punto necesita una tercera subred. La figura muestra los números de subred, máscaras y rango de direcciones. Observe que todas las direcciones y subredes son parte de la misma y única red con clase de Clase B 172.16.0.0, y todas las subredes usan la máscara 255.255.255.0.

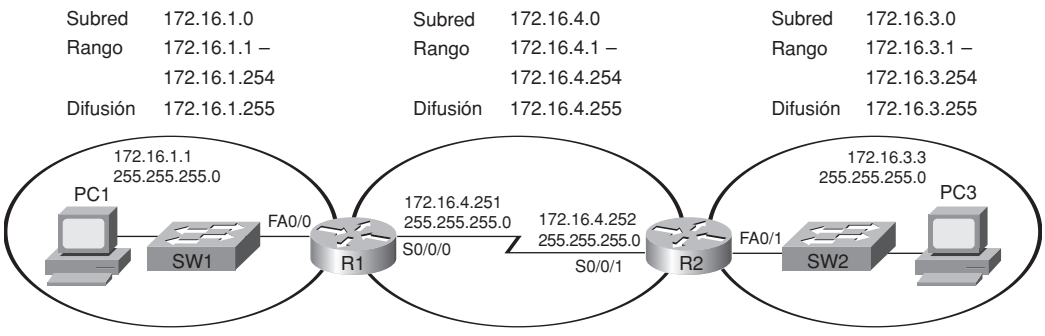


Figura 4.3. Ejemplo de diseño de direccionamiento IP.

La Figura 4.3 muestra los números de subred, rango de direcciones y dirección de difusión de la subred. Sin embargo, cada dispositivo de la figura puede encontrar la misma información basándose en su respectiva configuración de dirección IP y máscara de subred, derivando el número de subred, el rango de direcciones y la dirección de difusión para cada subred conectada.

Los exámenes CCNA requieren del dominio de los conceptos de direccionamiento y *subnetting* IP, pero más significativo, el examen requiere el dominio de la matemática usada para analizar las redes IP existentes y diseñar nuevas redes IP. Si no ha tenido tiempo de dominar las subredes, sería útil estudiar y practicar antes de avanzar en su lectura. Aunque esta sección ha revisado lo básico del direccionamiento IP, no trata la matemática de *subnetting*.

Para aprender sobre *subnetting* y la matemática relacionada, tiene un par de opciones. Aquellos que también han comprado el libro *CCENT/CCNA ICND1 Guía oficial para el examen de certificación*, deben profundizar en el Capítulo 12 de este libro y resolver los problemas prácticos listados. Para aquellos que han comprado este libro sin el libro ICND1, todos los recursos para aprender subredes del libro ICND1 han sido incluidos en el DVD de este libro. Refiérase a los siguientes elementos:

- Apéndice D, "Práctica de subnetting", sólo en el DVD.
- Apéndice E, "Páginas de referencia de *subnetting*", sólo en el DVD.
- Apéndice H, "Capítulo 12 de ICND1: Direccionamiento y *subnetting* IP", sólo en el DVD.
- Vídeos de *subnetting*.

Para continuar con la lectura del resto de este libro sin permitir que la matemática de subredes cause cualquier dificultad, debe ser capaz de hacer las tareas de la siguiente lista, tomándose el tiempo necesario. No ha de encontrar las respuestas rápidamente en este punto de su preparación, pero para estar preparado para los exámenes, debería completar las tareas en el límite de tiempo indicado:

- Dada una máscara en formato decimal con puntos, convertirla a notación con prefijo, o viceversa. (Tiempo sugerido para contestar en el examen: 5 segundos.)
- Dada una dirección IP y una máscara, encontrar el número de subred, el rango de direcciones y la dirección de difusión de la subred. (Tiempo sugerido: 15 segundos.)
- Dada una máscara de subred y la clase (A, B o C) de una red, determinar el número de subredes y hosts por subred. (Tiempo sugerido: 15 segundos.)
- Dada una clase de red (A, B o C) y los requisitos de diseño para un número de subredes y número de hosts por subred, encontrar todas las máscaras que reúnan los requisitos, y elegir la máscara que maximice el número de subredes o el número de hosts por subred. (Tiempo sugerido: 30 segundos.)
- Dada una red con clase y una única máscara de subred para usar en todas las subredes, listar los números de subred, e identificar la subred cero y la subred de difusión. (Tiempo sugerido: 30 segundos.)

Con estos detalles de subredes en mente, la siguiente sección examina cómo un router selecciona la ruta de la tabla de enrutamiento cuando las subredes listadas en la tabla se solapan porque la dirección de destino de un paquete coincide con más de una ruta.

Envío IP por la ruta más específica

Cualquier proceso de enrutamiento IP de router requiere que el router compare la dirección IP de destino de cada paquete con el contenido existente en la tabla de enrutamiento IP de ese router. A menudo, sólo una ruta coincide con una dirección de destino particular. Sin embargo, en algunos casos, una dirección de destino particular coincide con más de una ruta del router. Algunas razones legítimas y normales para el solapamiento de rutas en una tabla de enrutamiento son las siguientes:

- El uso de autoresumen.
- Resumen manual de rutas.
- El uso de rutas estáticas.
- Diseños incorrectos de subredes de forma que las subredes solapen sus rangos de direcciones.

El capítulo 5, "VLSM y resumen de rutas", explica más detalles acerca de cada una de estas razones. Mientras algunos casos de solapamiento de rutas son problemas, otros casos son resultado de una operación normal resultado de alguna otra característica. Esta sección se centra en cómo un router elige cuál de las rutas solapadas utilizar; las características que provocan el solapamiento se tratarán en el Capítulo 5.

La siguiente frase resume la lógica de envío de un router con rutas solapadas:

> Cuando una dirección IP de destino particular coincide con más de una ruta de la tabla de enrutamiento, el router utiliza la ruta más específica; con otras palabras, la ruta con mayor longitud de prefijo.

Para ver qué significa esto exactamente, la tabla de enrutamiento del Ejemplo 4.1 muestra una serie de rutas solapadas. Primero, antes de leer el texto que sigue al ejemplo, trate de predecir qué ruta podría utilizarse para enviar paquetes a las siguientes direcciones IP: 172.16.1.1, 172.16.1.2, 172.16.2.3 y 172.16.4.3.

Ejemplo 4.1. Comando **show ip route** con rutas solapadas.

```
R1#show ip route rip

     172.16.0.0/16 is variably subnetted, 5 subnets, 4 masks
R       172.16.1.1/32 [120/1] via 172.16.25.2, 00:00:04, Serial0/1/1
R       172.16.1.0/24 [120/2] via 172.16.25.129, 00:00:09, Serial0/1/0
R       172.16.0.0/22 [120/1] via 172.16.25.2, 00:00:04, Serial0/1/1
R       172.16.0.0/16 [120/2] via 172.16.25.129, 00:00:09, Serial0/1/0
R       0.0.0.0/0 [120/3] via 172.16.25.129, 00:00:09, Serial0/1/0
R1#show ip route 172.16.4.3
Routing entry for 172.16.0.0/16
  Known via "rip", distance 120, metric 2
  Redistributing via rip
  Last update from 172.16.25.129 on Serial0/1/0, 00:00:19 ago
  Routing Descriptor Blocks:
  * 172.16.25.129, from 172.16.25.129, 00:00:19 ago, via Serial0/1/0
      Route metric is 2, traffic share count is 1!
```

Aunque con la pregunta se podría suministrar un diagrama de la internetwork, realmente sólo se necesitan dos piezas de información para determinar qué ruta será elegida: la dirección IP de destino del paquete y el contenido de la tabla de enrutamiento del router. Examinando cada subred y máscara de la tabla de enrutamiento, se puede determinar el rango de direcciones IP en cada subred. En este caso, los rangos definidos por cada ruta, respectivamente, son los siguientes:

- 172.16.1.1 (exactamente esta dirección)
- 172.16.1.0–172.16.1.255
- 172.16.0.0–172.16.3.255
- 172.16.0.0–172.16.255.255
- 0.0.0.0–255.255.255.255 (todas las direcciones)

Nota

La ruta mostrada como 0.0.0.0/0 es la ruta predeterminada, que coincide con todas las direcciones IP, y se explica más adelante en este capítulo.

Como se puede ver en estos rangos, varios rangos de direcciones de rutas se solapan. Cuando coinciden más de una ruta, se utiliza la ruta con la mayor longitud de prefijo. Por ejemplo:

- **172.16.1.1:** Coincide con las cinco rutas; el prefijo más largo es /32, la ruta para 172.16.1.1/32.
- **172.16.1.2:** Coincide con las cuatro últimas rutas; el prefijo más largo es /24, la ruta para 172.16.1.0/24.
- **172.16.2.3:** Coincide con las tres últimas rutas; el prefijo más largo es /22, la ruta para 172.16.0.0/22.
- **172.16.4.3:** Coincide con las dos últimas rutas; el prefijo más largo es /16, la ruta para 172.16.0.0/16.

Además de mostrar las rutas a todas las subredes, el comando show ip route *dirección-ip* puede también ser particularmente útil. Este comando muestra información detallada acerca de la ruta que un router elegiría para la dirección IP listada en el comando. Si existen varias rutas que coinciden para esta dirección IP, este comando muestra la mejor de ellas: la ruta con el prefijo más largo. Por ejemplo, el Ejemplo 4.1 lista la salida del comando show ip route 172.16.4.3. La primera línea (sombreada) de la salida muestra la ruta elegida: la ruta para 172.16.0.0/16. El resto de la salida lista los detalles de ese router en particular. Este comando puede ser un comando práctico tanto en la vida real como para las preguntas de simulación de los exámenes.

DNS, DHCP, ARP e ICMP

El proceso de enrutamiento IP utiliza varios protocolos relacionados, incluyendo el protocolo ARP ya mencionado en este capítulo. Antes de continuar con el siguiente tema, esta sección revisa varios protocolos relacionados.

Antes de que un host pueda enviar cualquier paquete IP, necesita conocer varios parámetros relacionados con IP. Los hosts a menudo utilizan el Protocolo de configuración dinámica del host (DHCP, *Dynamic Host configuration Protocol*) para aprender estos factores clave, incluyendo:

- La dirección IP del host.
- La máscara de subred asociada.
- La dirección IP del gateway (router) predeterminado.
- La(s) dirección(es) del(de los) servidor(es) DNS.

Para aprender esta información, el host (un cliente DHCP) envía una difusión que eventualmente llega a un servidor DHCP. El servidor entonces alquila una dirección IP a este host y le proporciona el resto de información de la lista previa. En ese punto, el host tiene una dirección IP que usar como una dirección IP de origen, e información suficiente para tomar la sencilla decisión de enrutamiento de host de si enviar paquetes directamente a otro host (misma subred) o a su gateway predeterminado (otra subred). (En Windows XP de Microsoft, el comando `ipconfig/all` muestra las interfaces del host con la información listada antes de este párrafo.)

Típicamente el usuario directa o indirectamente se refiere a otro host por su nombre, lo cual a su vez provoca que el host necesite enviar un paquete a otro host. Por ejemplo, abrir un navegador web y teclear `http://www.cisco.com` donde el URL identifica el nombre de host de un servidor web propiedad de Cisco. Abriendo un cliente de correo electrónico como Microsoft Outlook indirectamente se referencia un nombre de host. El cliente de correo electrónico se configuró para conocer el nombre de host del servidor de correo entrante y saliente; así, aunque el usuario no mira estos valores todos los días, el software cliente de correo electrónico conoce el nombre de los hosts con los cuales intercambia correo.

Ya que los hosts no pueden enviar paquetes a un nombre de host de destino, la mayoría de los hosts utilizan los protocolos Sistema de denominación de dominio (DNS, *Domain Name System*) para resolver el nombre a su dirección IP asociada. El host actúa como cliente DNS, enviando mensajes a la dirección IP de unidifusión del servidor DNS. La solicitud DNS lista el nombre (por ejemplo, `www.cisco.com`) y el servidor contesta con la dirección IP que corresponde a ese nombre de host. Una vez aprendida, el host puede guardar en una caché la información "nombre a dirección", sólo necesaria para resolver ese nombre de nuevo antes de que la entrada caduque. (En Windows XP, el comando `ipconfig/displaydns` muestra la lista actual de nombres y direcciones del host.)

El Protocolo de mensajes de control en Internet (ICMP, *Internet Control Message Protocol*) incluye muchas funciones diferentes, todas centradas en el control y la gestión de IP. ICMP define un conjunto variado de mensajes para diferentes propósitos, incluyendo los mensajes de Petición y Respuesta de Eco. El popular comando `ping` valida la ruta a un host remoto, y la ruta inversa de vuelta al host original, enviando mensajes de Petición de Eco a la dirección IP de destino y con ese host de destino contestando a cada mensaje de Petición de Eco con un mensaje de Respuesta de Eco. Cuando el comando `ping` recibe los mensajes de Respuesta de Eco, el comando muestra que la ruta entre dos hosts funciona.

Todos estos protocolos trabajan juntos para ayudar al proceso de enrutamiento IP, pero DHCP, DNS, ICMP y ARP típicamente no ocurren para todos los paquetes. Por ejemplo, imagine un nuevo host conectado a una LAN, y el usuario teclea el comando ping www.cisco.com. DHCP podría haber sido usado en el arranque del SO, donde el PC utiliza DHCP para aprender su dirección IP y otra información, pero después DHCP podría no utilizarse durante días. El PC entonces utiliza DNS para resolver www.cisco.com en una dirección IP, pero después el PC no necesita usar DNS de nuevo hasta que se haga referencia a un nuevo nombre de host. Si el host hace ping al host remoto, el host local crea entonces un paquete IP, con una Petición de Eco ICMP en el paquete, con una dirección IP de destino de las direcciones aprendidas en la anterior petición DNS. Finalmente, como el host se acaba de encender, no tiene una entrada ARP para su gateway predeterminado, por lo que el host debe usar ARP para encontrar la dirección IP del gateway predeterminado. Sólo entonces puede el paquete ser entregado a su verdadero host de destino, como se ha descrito en la primera parte de este capítulo. Para los subsecuentes paquetes enviados al mismo nombre de host, esta sobrecarga de protocolos no será de nuevo necesaria, y el host local puede enviar el nuevo paquete.

La siguiente lista resume los pasos utilizados por un host, cuando es necesario, para los protocolos mencionados en esta sección:

1. Si no lo conoce todavía, el host utiliza DHCP para aprender su dirección IP, máscara de subred, direcciones IP de DNS, y dirección IP del gateway predeterminado. Si ya lo conoce, el host salta este paso.
2. Si el usuario referencia un nombre de host que no está en la actual caché de nombres del host, éste realiza una petición DNS para resolver el nombre a su correspondiente dirección IP. En otro caso, el host salta este paso.
3. Si el usuario ejecuta el comando ping, el paquete IP contiene una Petición de Eco ICMP; si el usuario en cambio utiliza una aplicación TCP/IP típica, utiliza los protocolos apropiados a esa aplicación.
4. Para construir la trama Ethernet, el host utiliza la entrada de la caché ARP para el dispositivo de siguiente salto: o bien el gateway predeterminado (cuando envía a un host de otra subred) o bien al verdadero host de destino (cuando envía a un host de la misma subred). Si la caché ARP no contiene esta entrada, el host utiliza ARP para aprender la información.

Fragmentación y MTU

TCP/IP define una longitud máxima de un paquete IP. El término utilizado para describir esta longitud máxima es **unidad máxima de transmisión** (MTU, *maximum transmission unit*).

La MTU varía en función de la configuración y las características de las interfaces. De forma predeterminada, una computadora calcula la MTU de una interfaz en función del tamaño máximo de la parte de datos de la trama de enlace de datos (donde el pa-

quete es colocado). Por ejemplo, el valor predeterminado de MTU en interfaces Ethernet es 1500.

Los routers, como cualquier host IP, no pueden reenviar paquetes por una interfaz si el paquete es más largo que la MTU. Si la MTU de interfaz de un router es menor que el paquete que debe ser enviado, el router fragmenta el paquete en paquetes más pequeños. La fragmentación es el proceso de fraccionar el paquete en paquetes más pequeños, cada uno de los cuales es menor o igual al valor de la MTU. La Figura 4.4 muestra un ejemplo de fragmentación en una red donde la MTU en el enlace serie ha sido bajada a 1000 bytes por configuración.

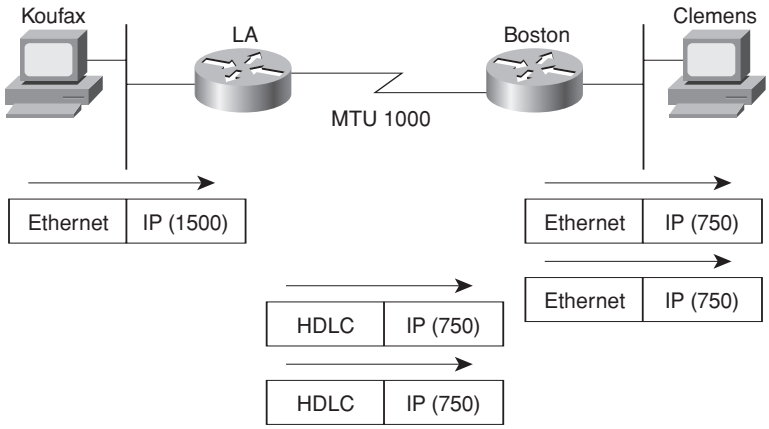


Figura 4.4. Fragmentación IP.

Como ilustra la Figura 4.4, Koufax envía un paquete de 1500 bytes al Router LA. LA elimina el encabezado Ethernet pero no puede enviar el paquete como es, porque es de 1500 bytes y el enlace de Control de enlace de datos de capa superior (HDLC, *High-Level Data Link Control*) sólo soporta una MTU de 1000. Por tanto, LA fragmenta el paquete original en dos paquetes, cada uno de 750 bytes de longitud. El router realiza los cálculos necesarios para obtener el menor número de fragmentos (dos en este caso) y divide el paquete original en dos paquetes de igual longitud. Por esto, será menos probable que cualquier otro router por el que pase el paquete necesite fragmentarlo de nuevo. Después de enviar los dos paquetes, Boston los recibe y los envía **sin reensamblarlos**. El reensamblado sólo lo realiza el host final, que en este caso es Clemens.

La cabecera IP contiene campos útiles para reensamblar los fragmentos y obtener el paquete original. La cabecera IP incluye un valor ID que es el mismo para cada fragmento del paquete, así como un valor de desplazamiento que define qué parte del paquete original contiene cada fragmento. Los paquetes fragmentados que llegan desordenados pueden ser identificados como una parte del mismo paquete original y pueden ser reensamblados en el orden correcto utilizando el campo de desplazamiento en cada fragmento.

Se pueden utilizar dos comandos de configuración para cambiar el tamaño de la MTU IP en una interfaz: los subcomandos de interfaz mtu e ip mtu. El comando mtu establece la MTU para todos los protocolos de capa 3; a menos que exista la necesidad de variar el valor para cada protocolo de capa 3, este comando es perfecto. Si se desea un valor diferente para IP, el comando ip mtu establece el valor a utilizar en IP. Si ambos se configuran en una interfaz, la configuración MTU de IP tiene preferencia en esta interfaz. Sin embargo, si el comando mtu se configura después de ip mtu, el valor de ip mtu se establece al mismo valor que el especificado en el comando mtu. Preste atención cuando cambie estos valores.

La revisión del enrutamiento y el direccionamiento IP está completa. A continuación, este capítulo examina las rutas conectadas, incluyendo las rutas conectadas relativas al *trunking* VLAN y las direcciones IP secundarias.

Rutas a subredes conectadas directamente

Un router añade automáticamente una ruta a su tabla de enrutamiento para las subredes conectadas a cada interfaz, asumiendo que los dos hechos siguientes son ciertos:

- La interfaz está en estado operativo; con otras palabras, el estado de la interfaz en el comando show interfaces presenta un estado de línea *up* y un estado de protocolo *up*.
- La interfaz tiene una dirección IP asignada, bien con el subcomando de interfaz ip address o utilizando los servicios de cliente DHCP.

El concepto de rutas conectadas es relativamente básico. El router por supuesto necesita conocer el número de subred utilizada en la red física conectada a cada una de sus interfaces, pero si la interfaz no está actualmente operativa, el router necesita eliminar la ruta de su tabla de enrutamiento. El comando show ip route lista estas rutas con una *c* como código de ruta, significando conectada, y el comando show ip route connected lista sólo las rutas conectadas.

Las siguientes secciones acerca de las rutas conectadas se centran en un par de variaciones en la configuración que afectan a dichas rutas, afectando también a cómo los routers envían los paquetes. El primer tema es relativo a una utilidad llamada direccionamiento IP secundario, mientras que la segunda es relativa a la configuración de un router cuando se utiliza el *trunking* VLAN.

Direccionamiento IP secundario

Imagine que planifica su esquema de direccionamiento IP para una red. Más tarde, una subred en concreto crece, y ya ha utilizado todas las direcciones IP válidas en la subred. ¿Qué puede hacer? Existen tres opciones principales:

- Hacer la subred existente más grande.
- Migrar los hosts para que usen direcciones de otra subred diferente y más grande.
- Utilizar el direccionamiento secundario.

Todas las opciones son razonables, pero todas tienen algún problema.

Hacer la subred más grande, cambia la máscara utilizada en esta subred. Sin embargo, cambiar la máscara podría crear subredes solapadas. Por ejemplo, si la subred 10.1.4.0/24 se está quedando sin direcciones, y se hace un cambio a la máscara 255.255.254.0 (9 bits de host, 23 bits red/subred), la nueva subred incluye las direcciones 10.1.4.0 a 10.1.5.255. Si la subred 10.1.5.0/24 ya estaba asignada, con direcciones asignables de 10.1.5.1 hasta 10.1.5.254, se crearía un solapamiento, que no está permitido. Sin embargo, si las direcciones 10.1.5.x no se utilizan, expandir la vieja subred podría ser razonable.

La segunda opción es simplemente elegir una subred nueva, no utilizada, pero más grande. Podría ser necesario cambiar todas las direcciones IP. Es un proceso relativamente sencillo si la mayoría o todos los hosts utilizan DHCP, pero un proceso potencialmente laborioso si muchos hosts utilizan direcciones IP configuradas estáticamente.

Observe que las dos primeras soluciones implican la estrategia de usar diferentes máscaras en diferentes partes de la red. El uso de estas máscaras diferentes se denomina **máscaras de subred de longitud variable** (VLSM, *variable-length subnet masking*), que introduce más complejidad en la red, en especial para las personas que la monitorizan y resuelven los problemas de la red.

La tercera opción es usar la característica de enrutamiento de Cisco llamada **direccionamiento IP secundario**. El direccionamiento secundario utiliza múltiples redes o subredes en el mismo enlace de datos. Utilizando más de una subred en el mismo medio, se incrementa el número de direcciones IP disponibles. Para hacer que funcione, el router necesita una dirección IP en cada subred, así como que los hosts de cada subred tengan una dirección IP utilizable del gateway predeterminado en la misma subred. Además, los paquetes que necesiten pasar entre estas subredes deben ser enviados al router. Por ejemplo, la Figura 4.5 tiene la subred 10.1.2.0/24; asumamos que tiene todas sus direcciones IP asignadas. Asumiendo que la solución elegida es el direccionamiento secundario, la subred 10.1.7.0/24 también podría usarse en la misma Ethernet. El Ejemplo 4.2 muestra la configuración para el direccionamiento IP secundario en Yosemite.

El router tiene rutas conectadas para las subredes 10.1.2.0/24 y 10.1.7.0/24; por tanto, puede enviar paquetes a cada subred. Los hosts en cada subred en la misma LAN pueden utilizar 10.1.2.252 ó 10.1.7.252 como sus direcciones IP de gateway predeterminado, dependiendo de la subred en la que se encuentren.

Lo más negativo del direccionamiento secundario es que los paquetes enviados entre hosts de una LAN podrían ser ineficientemente enrutados. Por ejemplo, cuando un host en la subred 10.1.2.0 envía un paquete a un host en 10.1.7.0, la lógica del host emisor es enviar el paquete a su gateway predeterminado, porque el destino está en una subred diferente. Así, el host emisor envía el paquete al router, que después envía el paquete de vuelta a la misma LAN.

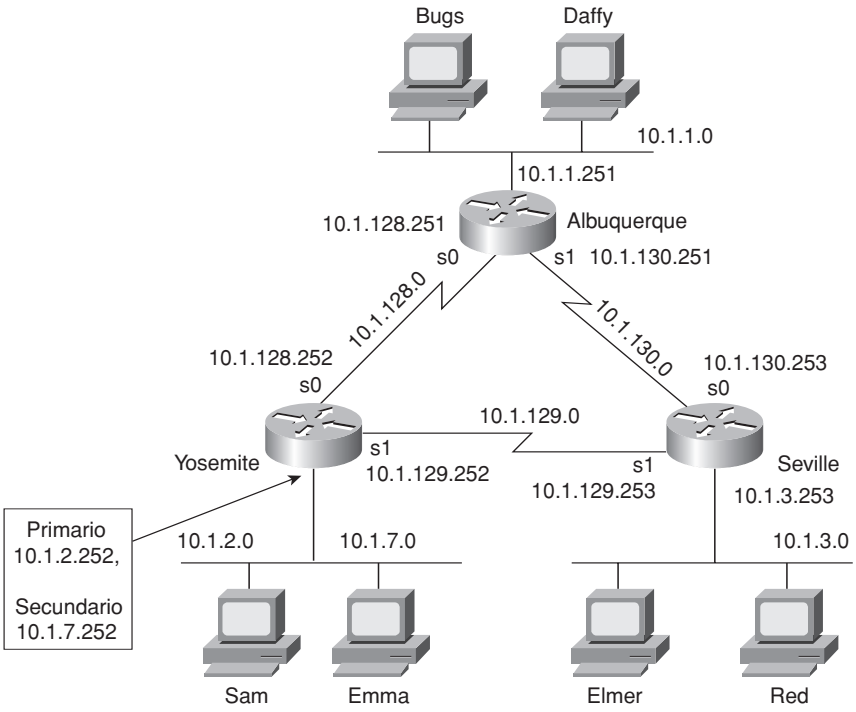


Figura 4.5. Red TCP/IP con direccionamiento secundario.

Ejemplo 4.2. Configuración de direccionamiento IP secundario y el comando **show ip route** en Yosemite.

```
! Extracto de show running-config a continuación...
Hostname Yosemite
ip domain-lookup
ip name-server 10.1.1.100 10.1.2.100
interface ethernet 0
 ip address 10.1.7.252 255.255.255.0 secondary
 ip address 10.1.2.252 255.255.255.0
interface serial 0
 ip address 10.1.128.252 255.255.255.0
interface serial 1
 ip address 10.1.129.252 255.255.255.0

Yosemite# show ip route connected
     10.0.0.0/24 is subnetted, 4 subnets
C       10.1.2.0 is directly connected, Ethernet0
C       10.1.7.0 is directly connected, Ethernet0
C       10.1.129.0 is directly connected, Serial1
C       10.1.128.0 is directly connected, Serial0
```

Soporte de rutas conectadas en la subred cero

El IOS puede restringir a un router configurar un comando ip address con una dirección dentro de la subred cero. La subred cero es una subred de cada red con clase que tiene todos ceros binarios en la parte de subred de la versión binaria de un número de subred. En decimal, sucede que la subred cero es el mismo número que el número de red con clase.

Con el comando configurado ip subnet-zero, el IOS permite que la subred cero llegue a ser una ruta conectada como resultado de un comando ip address configurado en una interfaz. Este comando ha sido una configuración predeterminada desde al menos la versión 12.0 del IOS, que será una versión de IOS relativamente antigua cuando este libro sea publicado. Por tanto, para el examen, si ve el comando ip subnet-zero configurado, o si la pregunta no especifica que el comando no ip subnet-zero está configurado, asuma que la subred cero puede ser configurada.

Nota

Las ediciones anteriores de este libro declaraban que se debería asumir que la subred cero no puede ser utilizada, a menos que una pregunta del examen implicara que la subred cero sí fuera utilizable. Los exámenes de CCNA actuales, y por tanto este libro, permiten que la subred cero sea utilizada a menos que la pregunta del examen afirme o implique que no pueda serlo.

Con el comando no ip subnet-zero configurado en un router, este router rechaza cualquier comando ip address que utilice una combinación dirección/máscara para la subred cero. Por ejemplo, el subcomando de interfaz ip address 10.0.0.1 255.255.255.0 implica la subred cero 10.0.0.0/24; por tanto, el router podría rechazar el comando si se configuró el comando de configuración global no ip subnet-zero. Observe que el mensaje de error diría simplemente "bad mask", en lugar de afirmar que el problema fue por la subred zero.

El comando no ip subnet-zero en un router no afecta a los otros routers, y no previene a un router de aprender acerca de la subred cero a través de un protocolo de enrutamiento. Él simplemente previene al router de configurar una interfaz en la subred cero.

Observe que en los exámenes actuales de CCNA, se puede asumir que puede utilizarse la subred cero a menos que la pregunta establezca que no lo será. En concreto, una pregunta que utilice un protocolo de enrutamiento con clase (como se discute en el Capítulo 5), o utilice el comando no ip subnet-zero, implica que las subredes cero y difusión deben evitarse.

Configuración de ISL y 802.1Q en los routers

Como se discutió en el Capítulo 1, el *trunking* VLAN se puede usar entre dos switches y entre un switch y un router. Mediante el uso del *trunking* en lugar de una interfaz física de router por VLAN, se puede reducir el número de interfaces de router necesarias. En vez

de una única interfaz física de router para cada VLAN en el switch, se puede utilizar una interfaz física, y el router todavía podrá enrutar paquetes entre las diferentes VLANs.

La Figura 4.6 muestra un router con una única interfaz Fast Ethernet y una única conexión a un switch. Se puede utilizar el *trunking* Enlace entre switches (ISL, *Inter-Switch Link*) o 802.1Q, con sólo pequeñas diferencias en la configuración de cada uno. Para tramas que contengan paquetes que el router enruta entre dos VLANs, la trama entrante es etiquetada por el switch con un ID VLAN, y la trama saliente es etiquetada por el router con el otro ID VLAN. El Ejemplo 4.3 muestra la configuración necesaria del router para soportar la encapsulación ISL y enviar entre estas VLANs.

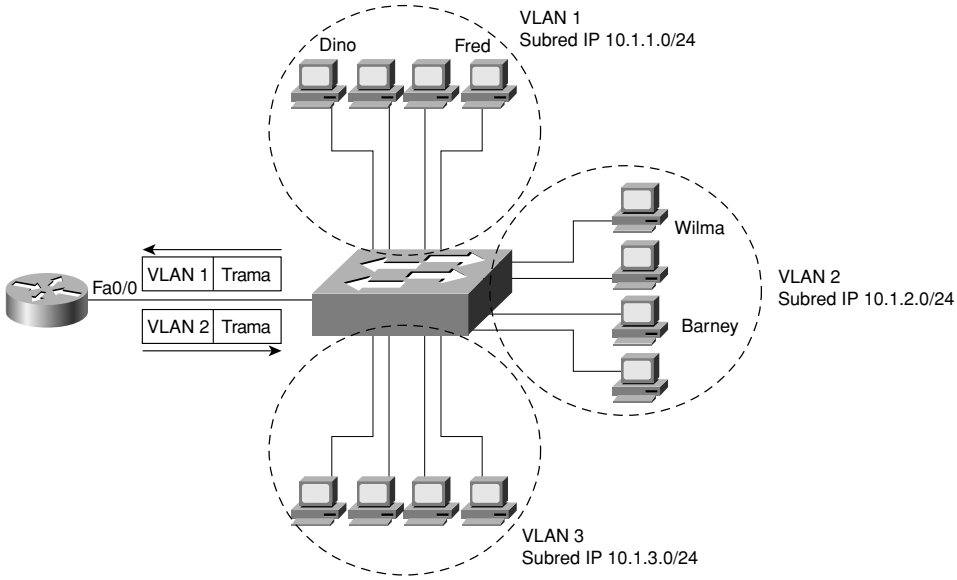


Figura 4.6. Router enviando entre VLANs.

Ejemplo 4.3. Configuración del router para la encapsulación ISL mostrada en la Figura 4.6.

```
interface fastethernet 0/0.1
 ip address 10.1.1.1 255.255.255.0
 encapsulation isl 1
!
interface fastethernet 0/0.2
 ip address 10.1.2.1 255.255.255.0
 encapsulation isl 2
!
interface fastethernet 0/0.3
 ip address 10.1.3.1 255.255.255.0
 encapsulation isl 3
```

El Ejemplo 4.3 muestra la configuración de tres subinterfaces de la interfaz Fast Ethernet del router. Una subinterfaz es una subdivisión lógica de una interfaz física. El router asigna a cada subinterfaz una dirección IP y asigna la subinterfaz a una única VLAN. Así, en vez de tres interfaces físicas de router, cada una conectada a una subred/VLAN diferente, el router utiliza una interfaz física de router con tres subinterfaces lógicas, cada una en una subred/VLAN diferente. El comando encapsulation numera las VLANs, que debe coincidir con la configuración de los IDs VLAN en el switch.

Este ejemplo utiliza números de subinterfaz que coinciden con el ID VLAN en cada subinterfaz. No es obligatorio que los números coincidan, pero muchas personas eligen hacerlo así, para hacer la configuración más obvia y facilitar la resolución de problemas. Dicho de otra forma, los IDs VLAN pueden ser 1, 2 y 3, pero los números de subinterfaz podrían ser 4, 5 y 6, ya que los números de subinterfaz sólo se usan internamente por el router.

El Ejemplo 4.4 muestra la misma red, pero ahora con 802.1Q en lugar de ISL. IEEE 802.1Q tiene un concepto llamado VLAN nativa, que es una VLAN especial en cada troncal para la cual no se añade una cabecera 802.1Q a las tramas. De forma predeterminada, VLAN 1 es la VLAN nativa. El Ejemplo 4.4 muestra la diferencia de configuración.

Ejemplo 4.4. Configuración del router para la encapsulación 802.1Q mostrada en la Figura 4.6.

```
interface fastethernet 0/0
 ip address 10.1.1.1 255.255.255.0
!
interface fastethernet 0/0.2
 ip address 10.1.2.1 255.255.255.0
 encapsulation dot1q 2
!
interface fastethernet 0/0.3
 ip address 10.1.3.1 255.255.255.0
 encapsulation dot1q 3
```

La configuración crea tres VLANs en la interfaz Fa0/0 del router. Dos de las VLANs, VLANs 2 y 3, se configuran como en el Ejemplo 4.3, excepto que el comando encapsulation muestra 802.1Q como el tipo de encapsulación.

La VLAN nativa, VLAN 1 en este caso, puede ser configurada con dos estilos de configuración. El Ejemplo 4.4 muestra un estilo en el cual la dirección IP de la VLAN nativa se configura en la interfaz física. Como resultado, el router no utiliza cabeceras de *trunking* en esta VLAN, como se quiere para la VLAN nativa. La alternativa es configurar la dirección IP de la VLAN nativa en otra subinterfaz y utilizar el subcomando de interfaz encapsulation dot1q 1 native. Este comando le dice al router que la subinterfaz está asociada con VLAN 1, pero la palabra clave native le dice al router que no utilice ningún encabezado 802.1Q en esta subinterfaz.

Los routers no realizan la negociación dinámica del *trunking*. Por tanto, el switch conectado a una interfaz de un router debe configurar manualmente el *trunking*, como se ha tratado en el Capítulo 1. Por ejemplo, un switch en el otro extremo de la interfaz Fa0/0 del router

podría configurar el subcomando de interfaz switchport mode trunk (para habilitar el *trunking* manualmente), y si el switch es capaz de utilizar otro tipo de *trunking*, el subcomando de interfaz switchport trunk encapsulation dot1q para configurar estáticamente el uso de 802.1Q.

Rutas estáticas

Los routers utilizan tres métodos para añadir rutas a sus tablas de enrutamiento: rutas conectadas, rutas estáticas y protocolos de enrutamiento dinámico. Los routers siempre añaden las rutas conectadas cuando las interfaces tienen direcciones IP configuradas y las interfaces están *up* y funcionando. En la mayoría de las redes, los ingenieros utilizan deliberadamente protocolos de enrutamiento dinámico para provocar que cada router aprenda el resto de rutas en la internetwork. Las rutas estáticas (rutas añadidas en la tabla de enrutamiento a través de configuración directa) es la menos usada de las tres opciones.

Las rutas estáticas constan de comandos de configuración global ip route individuales que definen una ruta para un router. El comando de configuración incluye una referencia a la subred (el número de subred y la máscara) junto con instrucciones acerca de dónde enviar paquetes destinados a esa subred. Para ver la necesidad de las rutas estáticas y su configuración, consultar el Ejemplo 4.5 que muestra dos comandos ping verificando la conectividad IP desde Alburquerque a Yosemite (véase la Figura 4.7).

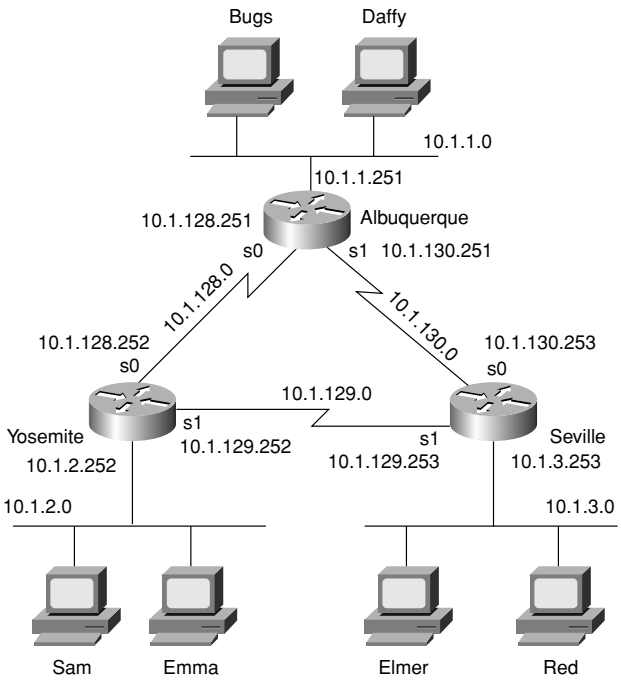


Figura 4.7. Red de ejemplo utilizada en los ejemplos de configuración de rutas estáticas.

Ejemplo 4.5. Comandos EXEC en el router Albuquerque con sólo rutas conectadas.

```
Albuquerque#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 3 subnets

C        10.1.1.0 is directly connected, Ethernet0
C        10.1.130.0 is directly connected, Serial1
C        10.1.128.0 is directly connected, Serial0
Albuquerque#ping 10.1.128.252
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.128.252, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

Albuquerque#ping 10.1.2.252
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.252, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

El final del ejemplo muestra dos comandos ping diferentes en el router Albuquerque, uno a 10.1.128.252 (dirección IP de S0 de Yosemite) y otra a 10.1.2.252 (dirección IP LAN de Yosemite). El comando IOS ping envía cinco paquetes de petición de eco ICMP de forma predeterminada, con la salida del comando mostrando una exclamación (!) que significa que la petición de eco se recibió, y un punto (.) para significar que no se recibió ningunas respuesta. En el ejemplo, la primera instancia, ping 10.1.128.252, muestra cinco respuestas (100%), y la segunda, ping 10.1.2.252, muestra que no se han recibido respuestas (0%). El primer comando ping funciona porque Albuquerque tiene una ruta a la subred en la que está 10.1.128.2 (subred 10.1.128.0/24). Sin embargo, el ping a 10.1.2.252 no funciona porque Albuquerque no tiene una ruta que coincida con la dirección 10.1.2.252. En este punto, Albuquerque sólo tiene rutas para sus tres subredes conectadas. Por tanto, el comando de Albuquerque ping 10.1.2.252 crea los paquetes, pero Albuquerque descarta los paquetes porque no existe rutas.

Configuración de rutas estáticas

Una solución sencilla para este fallo del comando ping 10.1.2.252 es habilitar un protocolo de enrutamiento IP en los tres routers. De hecho, en una red real, ésta es la solución

más probable. Como una alternativa, se pueden configurar rutas estáticas. La mayoría de las redes tienen pocas rutas estáticas, por lo que será necesario configurarlas ocasionalmente. El Ejemplo 4.6 muestra el comando ip route en Albuquerque, que añade rutas estáticas y hace que el ping fallido del Ejemplo 4.5 funcione.

Ejemplo 4.6. Rutas estáticas añadidas a Albuquerque.

```
ip route 10.1.2.0 255.255.255.0 10.1.128.252
ip route 10.1.3.0 255.255.255.0 10.1.130.253
```

El comando ip route define la ruta estática con el número de subred y la dirección IP del siguiente salto. Un comando ip route define una ruta a 10.1.2.0 (máscara 255.255.255.0), que está localizada en Yosemite; así, la dirección IP del siguiente salto configurada en Albuquerque es 10.1.128.252, que es la dirección IP de Serial0 de Yosemite. De forma similar, una ruta a 10.1.3.0, la subred de Seville, apunta a la dirección IP de Serial0 de Seville, 10.1.130.253. Observe que la dirección IP de siguiente salto es una dirección IP en una subred directamente conectada; el objetivo es definir el siguiente router al que enviar el paquete. Ahora, Albuquerque puede enviar paquetes a estas dos subredes.

El comando ip route tiene dos formatos básicos. El comando puede referirse a la dirección IP del siguiente salto, como se muestra en el Ejemplo 4.6. Alternativamente, para rutas estáticas que utilizan enlaces serie punto a punto, el comando puede mostrar la interfaz de salida en vez de la dirección IP del siguiente salto. Por ejemplo, el Ejemplo 4.6 podría en cambio utilizar el comando de configuración global ip route 10.1.2.0 255.255.255.0 serial0 en lugar del primer comando ip route.

Desafortunadamente, añadir las dos rutas estáticas en el Ejemplo 4.6 para Albuquerque no soluciona todos los problemas de enrutamiento de la red. Las rutas estáticas ayudan a Albuquerque a entregar paquetes a las otras dos subredes, pero los otros dos routers no tienen suficiente información para enviar paquetes de vuelta a Albuquerque. Por ejemplo, el PC Bugs no puede hacer *ping* al PC Sam en esta red, incluso después de añadir los comandos del Ejemplo 4.6. El problema es que aunque Albuquerque tiene una ruta a la subred 10.1.2.0, a la que Sam pertenece, Yosemite no tiene ruta a 10.1.1.0, donde está Bugs. El paquete de petición de ping va de Bugs a Sam correctamente, pero el paquete de respuesta al *ping* de Sam no puede ser enrutado por el router Yosemite de vuelta a través de Albuquerque a Bugs; por tanto, el *ping* falla.

El comando Ping extendido

En la vida real, puede pasar que no se pueda encontrar a un usuario, como Bugs, para verificar la red con el comando ping. En cambio, se puede utilizar el comando ping extendido en un router para verificar el enrutamiento de la misma manera que lo haría un *ping* desde Bugs hasta Sam. El Ejemplo 4.7 muestra Albuquerque con el comando ping 10.1.2.252 funcionando, pero con un comando ping 10.1.2.252 extendido que funciona de

forma similar a un ping desde Bugs hasta Sam, un *ping* que falla en este caso (en este punto sólo se han añadido las dos rutas estáticas del Ejemplo 4.6).

Ejemplo 4.7. Albuquerque: Ping funcionando después de añadir las rutas predeterminadas, más el comando **ping** extendido fallido.

```
Albuquerque#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 5 subnets
S        10.1.3.0 [1/0] via 10.1.130.253
S        10.1.2.0 [1/0] via 10.1.128.252
C        10.1.1.0 is directly connected, Ethernet0
C        10.1.130.0 is directly connected, Serial1
C        10.1.128.0 is directly connected, Serial0
Albuquerque#ping 10.1.2.252

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.252, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

Albuquerque#ping
Protocol [ip]:
Target IP address: 10.1.2.252
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.251
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.252, timeout is 2 seconds:
. . . . .
Success rate is 0 percent (0/5)
```

El comando ping 10.1.2.252 funciona por una razón obvia y una no tan obvia. Primero, Albuquerque puede enviar un paquete a la subred 10.1.2.0 por la ruta estática. El paquete de vuelta, enviado por Yosemite, es enviado a la dirección 10.1.128.251 (dirección IP de Serial0 en Albuquerque) y Yosemite tiene una ruta conectada para alcanzar la subred 10.2.128.0. Pero ¿Por qué Yosemite envía la respuesta de eco a la dirección IP S0 de Albuquerque 10.1.128.251? Bien, los siguientes puntos son verdaderos acerca del comando ping en un router de Cisco:

- El comando ping de Cisco utiliza, de forma predeterminada, la dirección IP de la interfaz de salida como dirección de origen del paquete, a menos que se especifique otra cosa en un ping extendido. El primer ping en el Ejemplo 4.7 utiliza un origen de 10.1.128.251, porque la ruta utilizada para enviar el paquete a 10.1.2.252 envía paquetes por la interfaz Serial0 de Albuquerque, cuya dirección IP es 510.1.128.251.
- Los paquetes de respuesta (respuesta de eco ICMP) invierten las direcciones IP utilizadas en la petición *ping* recibida al contestar. Así, en este ejemplo, la respuesta de eco de Yosemite, en respuesta al primer ping del Ejemplo 4.7, utiliza 10.1.128.251 como la dirección de destino y 10.1.2.252 como la dirección IP de origen.

Como el comando ping 10.1.2.252 en Albuquerque utiliza 10.1.128.251 como dirección de origen del paquete, Yosemite puede enviar una respuesta a 10.1.128.251, porque Yosemite pasa por tener una ruta (conectada) a 10.1.128.0.

El peligro al resolver problemas con el comando estándar ping es que los problemas de enrutamiento pueden existir todavía, pero el comando ping 10.1.2.252, que funciona, proporciona una falsa sensación de seguridad. Una alternativa más completa es utilizar el comando ping extendido para actuar como si se ejecutara un ping desde una computadora de esa subred, sin tener que llamar a un usuario y pedirle que ejecute por usted el comando ping en el PC. La versión extendida del comando ping puede utilizarse para refinar la causa del problema subyacente cambiando varios detalles de lo que el comando ping envía en sus peticiones. De hecho, cuando un ping desde un router funciona, pero un ping desde un host no lo hace, el comando ping extendido podría ayudar a recrear el problema sin necesidad de trabajar con el usuario final hablando por teléfono.

Por ejemplo, en el Ejemplo 4.7, el comando ping extendido en Albuquerque envía un paquete desde la dirección IP de origen 10.1.1.251 (la Ethernet de Albuquerque) a 10.1.2.252 (la Ethernet de Yosemite). Acorde con la salida, Albuquerque no recibe una respuesta. Normalmente, el comando ping tendría el origen en la dirección IP de la interfaz de salida. Con el uso de la opción de la dirección de origen del ping extendido, la dirección IP de origen del paquete de eco se establece a la dirección IP de la Ethernet de Albuquerque, 10.1.1.251. Debido a que el eco ICMP generado por el ping extendido tiene como origen una dirección de la subred 10.1.1.0, el paquete se ve como un paquete desde un usuario final en esa subred. Yosemite construye una respuesta de eco, con destino 10.1.1.251, pero no hay una ruta para esta subred. Por tanto, Yosemite no puede enviar un paquete de respuesta al ping de Albuquerque.

Para solucionar este problema, todos los routers podrían configurarse para utilizar un protocolo de enrutamiento. Alternativamente, se podrían definir simplemente rutas estáticas en todos los routers de la red.

Rutas estáticas predeterminadas

Una ruta predeterminada es una ruta especial que coincide con todos los destinos de los paquetes. Las rutas predeterminadas pueden ser particularmente útiles cuando sólo existe un camino físico desde una parte de la red a otra, y en casos para los cuales un único router de la empresa proporciona conectividad a Internet para esta empresa. Por ejemplo, en la Figura 4.8, R1, R2 y R3 están conectados al resto de la red sólo a través de la interfaz LAN de R1. Los tres routers pueden enviar paquetes al resto de la red mientras alcancen R1, que a su vez enviará los paquetes al router Dist1.

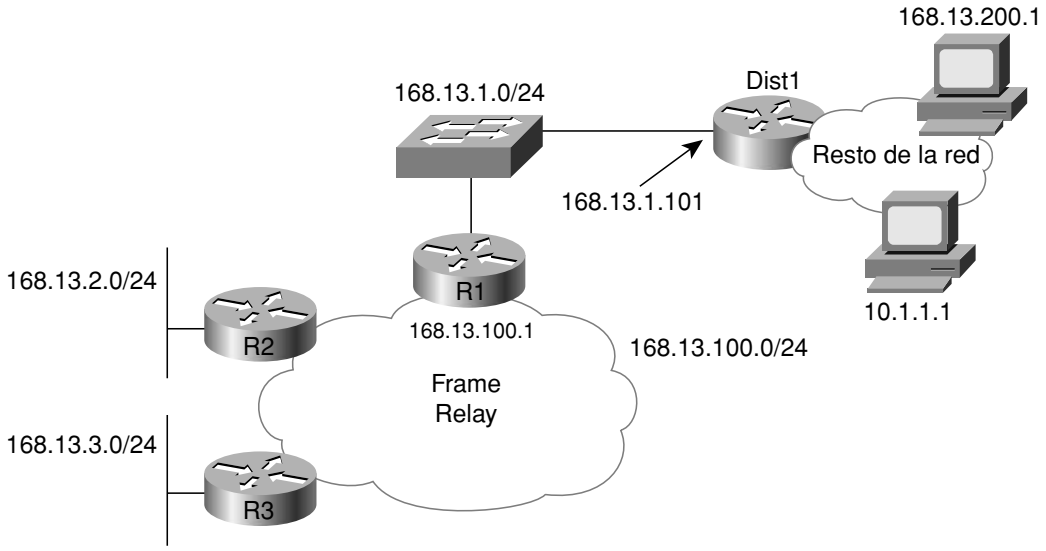


Figura 4.8. Red sencilla utilizando una ruta predeterminada.

Las siguientes secciones muestran dos opciones para configurar rutas estáticas predeterminadas: una utilizando el comando ip route y otra con el comando ip default-network.

Rutas predeterminadas empleando el comando ip route

Configurando una ruta predeterminada en R1, con el router Dist1 como siguiente salto, y R1 publicando a R2 y R3 la ruta predeterminada, se puede conseguir un enrutamiento predeterminado. Utilizando rutas predeterminadas, R1, R2 y R3 no necesitarían rutas específicas a las subredes a la derecha del router Dist1. El Ejemplo 4.8 comienza un examen de este diseño mostrando la definición de una ruta predeterminada estática en R1 y la información resultante en la tabla de enrutamiento IP de R1.

R1 define la ruta predeterminada con un comando ip route estático, con destino 0.0.0.0, máscara 0.0.0.0. Como resultado, el comando show ip route en R1 lista una ruta estática a 0.0.0.0, máscara 0.0.0.0, con siguiente salto 168.13.1.101 (esencialmente, la misma informa-

Ejemplo 4.8. Configuración de ruta predeterminada estática y tabla de enrutamiento en R1.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 168.13.1.101
R1#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 168.13.1.101 to network 0.0.0.0

      168.13.0.0/24 is subnetted, 4 subnets
C        168.13.1.0 is directly connected, FastEthernet0/0
R        168.13.3.0 [120/1] via 168.13.100.3, 00:00:05, Serial0.1
R        168.13.2.0 [120/1] via 168.13.100.2, 00:00:21, Serial0.1
C        168.13.100.0 is directly connected, Serial0.1
S*    0.0.0.0/0 [1/0] via 168.13.1.101
```

ción que el comando de configuración global ip route 0.0.0.0 0.0.0.0 168.13.1.101). Un destino de 0.0.0.0, con máscara 0.0.0.0, representa por convención todos los destinos. Con esta configuración, R1 tiene una ruta estática que coincide con cualquiera y con todos los destinos de un paquete IP.

Observe también en el Ejemplo 4.8 que la salida del comando show ip route en R1 muestra 168.13.1.101 como "gateway de último recurso". Cuando un router tiene conocimiento de la última ruta predeterminada, el router marca esta ruta con un asterisco en la tabla de enrutamiento. Si un router aprende varias rutas predeterminadas (bien por configuración estática o bien por protocolos de enrutamiento), el router marca cada ruta predeterminada con un asterisco en la tabla de enrutamiento. Entonces, el router elige la mejor de las rutas predeterminadas, anotando esta elección como gateway de último recurso. (La distancia administrativa del origen de la información de enrutamiento, definida por la configuración de distancia administrativa, tiene algo de impacto en esta elección. La distancia administrativa se trata en el Capítulo 8, "Teoría de los protocolos de enrutamiento", en la sección "Distancia administrativa".)

Aunque la configuración del Protocolo de información de enrutamiento (RIP, *Routing Information Protocol*) no se muestra, R1 también publica su ruta predeterminada a R2 y R3, como muestra la salida del comando show ip route en R3 en el Ejemplo 4.9.

Diferentes protocolos de enrutamiento publican rutas predeterminadas en un par de maneras diferentes. Como ejemplo, cuando R3 aprende una ruta predeterminada de R1 usando RIP, R3 muestra el destino de la ruta predeterminada (0.0.0.0) y el router de siguiente salto, que es R1 en este caso (168.13.100.1), como se resalta en el Ejemplo 4.9. Así, cuando R3 necesita usar su ruta predeterminada, enviará paquetes a R1 (168.13.100.1).

Ejemplo 4.9. Matices del uso satisfactorio de rutas estáticas en R1.

```
R3#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 168.13.100.1 to network 0.0.0.0

      168.13.0.0/24 is subnetted, 4 subnets
R        168.13.1.0 [120/1] via 168.13.100.1, 00:00:13, Serial0.1
C        168.13.3.0 is directly connected, Ethernet0
R        168.13.2.0 [120/1] via 168.13.100.2, 00:00:06, Serial0.1
C        168.13.100.0 is directly connected, Serial0.1
```

Rutas predeterminadas empleando el comando ip default-network

Otro estilo de configuración para la ruta predeterminada usa el comando ip default-network. Este comando tiene como parámetro una red IP con clase, diciéndole al router que utilice los detalles de enrutamiento de la ruta para esta red con clase como los detalles de envío para una ruta predeterminada.

Este comando es más útil cuando el ingeniero quiere utilizar una ruta predeterminada para alcanzar redes además de las redes usadas dentro de la empresa. Por ejemplo, en la Figura 4.8, imagine que todas las subredes de la red de clase B 168.13.0.0 de la empresa son conocidas; éstas existen sólo cerca de los routers R1, R2 y R3; y estos routers están todos en la tabla de enrutamiento de R1, R2 y R3. También, ninguna de las subredes de 168.1.0.0 está a la derecha del Router Dist1. Si el ingeniero quiere utilizar una ruta predeterminada para enviar paquetes a destinos a la derecha de Dist1, el comando ip default-network funciona bien.

Para usar el comando ip default-network para configurar una ruta predeterminada, el ingeniero cuenta con el conocimiento de que Dist1 está ya publicando una ruta para la red con clase 10.0.0.0 a R1. La ruta de R1 a la red 10.0.0.0 apunta a la dirección 168.13.1.101 de Dist1 como la dirección de siguiente salto. Conociendo esto, el ingeniero puede configurar el comando ip default-network 10.0.0.0 en R1, que le dice a R1 que construya su ruta predeterminada basándose en su ruta aprendida para la red 10.0.0.0/8. El Ejemplo 4.10 muestra varios detalles acerca de este escenario en R1.

R1 muestra el resultado de tener que aprender normalmente una ruta a la red 10.0.0.0 a través de RIP, más el resultado adicional del comando global ip default-network 10.0.0.0. La ruta RIP de R1 para 10.0.0.0/8 muestra una dirección IP de siguiente salto de 168.13.1.101, la dirección IP de Dist1 en su LAN común, como normal. Debido al coman-

Ejemplo 4.10. Uso del comando **ip default-network** en R1.

```
R1#configure terminal
R1(config)#ip default-network 10.0.0.0
R1(config)#exit
R1#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 168.13.1.101 to network 10.0.0.0

      168.13.0.0/24 is subnetted, 5 subnets
R        168.13.200.0 [120/1] via 168.13.1.101, 00:00:12, FastEthernet0/0
C        168.13.1.0 is directly connected, FastEthernet0/0
R        168.13.3.0 [120/1] via 168.13.100.3, 00:00:00, Serial0.1
R        168.13.2.0 [120/1] via 168.13.100.2, 00:00:00, Serial0.1
C        168.13.100.0 is directly connected, Serial0.1
R*    10.0.0.0/8 [120/1] via 168.13.1.101, 00:00:12, FastEthernet0/0
```

do ip default-network 10.0.0.0, R1 decide usar los detalles de la ruta a la red 10.0.0.0 como su ruta predeterminada. La última parte de la línea acerca del gateway de último recurso muestra la red predeterminada, 10.0.0.0. También, R1 muestra un asterisco antes de la ruta referenciada en el comando ip default-network.

Resumen de las rutas predeterminadas

Recordar los detalles de la configuración de rutas predeterminadas, y en particular los detalles del resultado de la salida del comando show ip route, puede ser un desafío. Sin embargo, hagamos un apunte para recordar estos puntos clave con respecto a las rutas predeterminadas:

- Las rutas predeterminadas estáticas se pueden configurar estáticamente utilizando el comando ip route 0.0.0.0 0.0.0.0 *dirección-siguiente-salto* o el comando ip default-network *número-red*.
- Cuando en un router un paquete sólo coincide con la ruta predeterminada, este router utiliza los detalles de envío mostrados en la línea de gateway de último recurso.

Sin tener en cuenta cómo se presenta la ruta predeterminada (si es un gateway de último recurso, una ruta 0.0.0.0, o una ruta a alguna otra red con un * al lado en la tabla de enrutamiento), se utiliza conforme a las reglas de enrutamiento con o sin clase, como se explica en la siguiente sección.

Enrutamiento con y sin clase

Los routers de Cisco tienen dos opciones configurables que influyen en cómo un router utiliza una ruta predeterminada existente: enrutamiento sin clase y enrutamiento con clase. El enrutamiento sin clase causa que un router utilice sus rutas predeterminadas para cualquier paquete que no coincida con ninguna otra ruta. El enrutamiento con clase coloca una restricción respecto a cuándo un router puede usar su ruta predeterminada, resultando en casos en los cuales un router tiene una ruta predeterminada pero el router elige descartar un paquete en lugar de enviarlo basándose en la ruta predeterminada.

Los términos **sin clase** y **con clase** también caracterizan el direccionamiento IP y los protocolos de enrutamiento IP; así existe una cierta confusión en el significado de los términos. Antes de explicar los detalles del enrutamiento con y sin clase, la siguiente sección resume el otro uso de estos términos.

Resumen del uso de los términos sin clase y con clase

Los términos **direccionamiento sin clase** y **direccionamiento con clase** se refieren a dos formas diferentes de pensar acerca de las direcciones IP. Ambos términos se refieren a una perspectiva de la estructura de dirección IP con subredes. El direccionamiento sin clase usa dos partes para ver las direcciones IP, y el direccionamiento con clase tiene una visión en tres partes. Con el direccionamiento con clase, la dirección siempre tiene un campo de red de 8, 16, ó 24 bits, basado en las reglas de direccionamiento de las Clases A, B y C. El final de la dirección tiene una parte de host que identifica cada host en una subred. Los bits entre la parte de red y de host forman la tercera parte, llamada parte de subred de la dirección. Con el direccionamiento sin clase, las partes de red y subred de la vista con clase se combinan en una única parte, llamada a menudo subred o prefijo, de modo que la dirección termina en la parte de host.

Los términos **protocolo de enrutamiento sin clase** y **protocolo de enrutamiento con clase** se refieren a características de los protocolos de enrutamiento IP diferentes. Estas características no pueden ser habilitadas o deshabilitadas; un protocolo de enrutamiento es, por su propia naturaleza, bien sin clase o bien con clase. En concreto, los protocolos de enrutamiento sin clase publican información de la máscara para cada subred, dando a los protocolos sin clase la habilidad de soportar VLSM y los resúmenes de rutas. Los protocolos con clase no publican información de la máscara; por tanto, no soportan VLSM o el resumen de rutas.

El tercer uso de los términos **sin clase** y **con clase** (los términos **enrutamiento con clase** y **enrutamiento sin clase**), tiene que ver con cómo el proceso de enrutamiento IP hace uso de la ruta predeterminada. De manera interesante, éste es el único de los tres usos de los términos con clase y sin clase que puede cambiar basándose en la configuración del router. La Tabla 4.2 lista los tres usos de los términos sin clase y con clase, con una breve explicación. Una explicación más completa del enrutamiento con y sin clase sigue a la tabla. El Capítulo 5 explica más fundamentos acerca de los términos **protocolo de enrutamiento sin clase** y **protocolos de enrutamiento con clase**.

Tabla 4.2. Comparando el uso de los términos sin clase y con clase.

Como aplicado a	Con clase	Sin clase
Direccionamiento	Las direcciones tienen tres partes: red, subred y host.	Las direcciones tienen dos partes: subred o prefijo, y host.
Protocolos de enrutamiento	El protocolo de enrutamiento no publica máscaras ni soporta VLSM; RIP-1 e IGRP.	El protocolo publica máscaras y soporta VLSM; RIP-2, EIGRP, OSPF.
Enrutamiento (envío)	El proceso de envío IP está restringido a cómo utiliza la ruta predeterminada.	El proceso de envío IP no tiene restricciones en el uso de la ruta predeterminada.

Comparación del enrutamiento con clase y sin clase

El enrutamiento IP sin clase funciona como la mayoría de las personas piensan que el enrutamiento IP podría funcionar cuando un router conoce una ruta predeterminada. Comparado con el enrutamiento con clase, los conceptos centrales del enrutamiento sin clase son directos. El enrutamiento con clase restringe el uso de la ruta predeterminada. Las dos sentencias siguientes ofrecen una descripción general de cada uno, con un ejemplo siguiendo a la definición:

- **Enrutamiento sin clase.** Cuando el destino de un paquete sólo coincide con la ruta predeterminada de un router, y no coincide con alguna otra ruta, envía el paquete utilizando esa ruta predeterminada.
- **Enrutamiento con clase.** Cuando el destino de un paquete sólo coincide con la ruta predeterminada de un router, y no coincide con alguna otra ruta, sólo utiliza la ruta predeterminada si este router no conoce cualquier ruta en la red con clase a la que pertenece la dirección IP de destino.

El uso del término **con clase** se refiere al hecho que la lógica incluye algunas consideraciones de reglas de direccionamiento IP con clase; a saber, la red con clase (Clases A, B o C) de la dirección de destino del paquete. Para ver el sentido de este concepto, el Ejemplo 4.11 muestra un router con una ruta predeterminada, pero el enrutamiento con clase permite el uso de la ruta predeterminada en un caso, pero no en otro. El ejemplo usa la misma ruta predeterminada de los ejemplos anteriores de este capítulo basados en la Figura 4.8. Ambos, R3 y R1, tienen una ruta predeterminada que podría enviar paquetes al router Dist1. Sin embargo, como se ve en el Ejemplo 4.11, en R3, el ping 10.1.1.1 funciona, pero el ping 168.13.200.1 falla.

Nota

Este ejemplo usa la ruta predeterminada en R1 como se ha definido con el comando ip route y explicado en los Ejemplos 4.8 y 4.9, pero podría haber funcionado de la misma forma independientemente de cómo se aprendiera la ruta predeterminada.

Ejemplo 4.11. El enrutamiento con clase causa un fallo del ping en R3.

```
R3#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 168.13.100.1 to network 0.0.0.0

      168.13.0.0/24 is subnetted, 4 subnets
R        168.13.1.0 [120/1] via 168.13.100.1, 00:00:13, Serial0.1
C        168.13.3.0 is directly connected, Ethernet0
R        168.13.2.0 [120/1] via 168.13.100.2, 00:00:06, Serial0.1
C        168.13.100.0 is directly connected, Serial0.1
R3#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/89/114 ms
R3#
R3#ping 168.13.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 168.13.200.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Primero, considerar que R3 está buscando ambos destinos (10.1.1.1 y 168.13.200.1) en la tabla de enrutamiento. La tabla de enrutamiento de R3 no tiene ninguna ruta que coincida con ninguna de las direcciones IP de destino, que no sea la ruta predeterminada. Por tanto, la única opción de R3 es utilizar su ruta predeterminada.

R3 está configurado para utilizar el enrutamiento con clase. Con dicho enrutamiento, el router primero busca el número de red de Clase A, B o C a la que pertenece el destino. Si se encuentra la red de Clase A, B o C, el IOS de Cisco busca entonces el número específico de subred. Si no se encuentra, el paquete es descartado, como en el caso de los ecos ICMP enviados con el comando ping 168.13.200.1. Sin embargo, con el enrutamiento sin clase, si el paquete no coincide con la red de Clase A, B o C en la tabla de enrutamiento, y existe una ruta predeterminada, la ruta predeterminada es de hecho utilizada; que es por lo que R3 puede enviar ecos ICMP satisfactoriamente con el comando ping 10.1.1.1.

En resumen, con el enrutamiento con clase, el único momento en que se utiliza la ruta predeterminada es cuando el router no conoce ninguna de las subredes de la red de Clase A, B o C de destino del paquete.

Se puede alternar el enrutamiento sin o con clase con los comandos de configuración global ip classless y no ip classless, respectivamente. Con el enrutamiento sin clase, el IOS de Cisco busca la mejor coincidencia, ignorando las reglas de clase. Si existe una ruta predeterminada, con el enrutamiento sin clase, el paquete siempre al menos coincide con la ruta predeterminada. Si una ruta más específica coincide con el destino del paquete, se usa esa ruta. El Ejemplo 4.12 muestra R3 cambiando para usar el enrutamiento sin clase, y el *ping* con éxito a 168.13.200.1.

Ejemplo 4.12. Enrutamiento sin clases permitiendo el *ping* a 168.13.200.1, ahora con éxito.

```
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip classless
R3(config)#^Z
R3#ping 168.13.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 168.13.200.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/88/112 ms
```

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. Tabla 4.3 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 4.3. Temas clave del Capítulo 4.

Tema clave	Descripción	Número de página
Lista	Pasos realizados por un host cuando envía paquetes IP.	162-163
Lista	Pasos realizados por un router cuando envía paquetes IP.	163
Lista	Revisión de los puntos clave del direccionamiento IP.	166-167
Razonamiento	Resumen de la lógica que un router utiliza cuando el destino de un paquete coincide con más de una ruta.	169
Lista	Elementos típicamente aprendidos a través de DHCP.	171
Lista	Pasos y protocolos utilizados por un host cuando se comunica con otro.	172
Lista	Reglas con respecto a cuándo un router crea una ruta conectada.	174
Lista	Reglas acerca de la dirección de origen utilizada en un paquete generado por el IOS con el comando ping.	184
Lista	Hechos clave relacionados con la definición de las rutas estáticas predeterminadas.	188
Tabla 4.2	Resumen de los tres separados pero relacionados usos de los términos sin clase y con clase.	190
Lista	Definiciones de enrutamiento sin clase y enrutamiento con clase.	190

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD) o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas ya completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe sus respuestas en el glosario:

Direccionamiento con clase, direccionamiento sin clase, dirección IP secundaria, enrutamiento con clase, enrutamiento sin clase, ping extendido, protocolo de enrutamiento con clase, protocolo de enrutamiento sin clase, subred cero.

Referencias de comandos

Aunque no necesariamente debe memorizar la información de las tablas de esta sección, ésta incluye una referencia de los comandos de configuración y EXEC utilizados en este capítulo. En la práctica, debería memorizar los comandos como un efecto colateral de leer el capítulo y hacer todas las actividades de esta sección de preparación del examen. Para verificar si ha memorizado los comandos como un efecto secundario de sus otros estudios, cubra el lado izquierdo de la tabla con un trozo de papel, lea las descripciones del lado derecho, y compruebe si recuerda el comando.

Tabla 4.4. Comandos de configuración del Capítulo 4.

Comando	Descripción
encapsulation dot1q *id-vlan* [native]	Un subcomando de interfaz que le dice al router que use el *trunking* 802.1Q, para una VLAN en concreto, y con la palabra clave native, para no encapsular en una cabecera de *trunking*.
encapsulation isl *identificador-vlan*	Un subcomando de interfaz que le dice al router que use el *trunking* ISL, para una VLAN particular.
[no] ip classless	Comando global que habilita (ip classless) o deshabilita (no ip classless) el enrutamiento sin clase.

(continúa)

Tabla 4.4. Comandos de configuración del Capítulo 4 *(continuación)*.

Comando	Descripción
[no] ip subnet-zero	Comando global que permite (ip subnet-zero) o prohíbe (no ip subnet-zero) la configuración de una dirección IP de una interfaz en la subred cero.
ip address *dirección-ip máscara* [secondary]	Subcomando de interfaz que asigna la dirección IP de una interfaz, y opcionalmente define a la dirección como secundaria.
ip route *prefijo máscara* {*dirección-ip* | *tipo-interfaz número-interfaz*} [*distancia*] [permanent]	Comando de configuración global que crea una ruta estática.
ip default-network *número-red*	Comando global que crea una ruta predeterminada basada en la ruta del router a la red con clase especificada en el comando.

Tabla 4.5. Comandos EXEC del Capítulo 4.

Comando	Descripción
show ip route	Muestra la tabla de enrutamiento completa de un router.
show ip route *dirección-ip*	Lista información detallada acerca de la ruta que un router selecciona para la dirección IP indicada.
ping {*nombre-host* | *dirección-ip*}	Verifica las rutas IP enviando paquetes ICMP al host destinatario.
traceroute {*nombre-host* | *dirección-ip*}	Verifica rutas IP descubriendo las direcciones IP de las rutas entre un router y el destino listado.

Este capítulo trata los siguientes temas:

VLSM: Esta sección explica los problemas y soluciones cuando se diseña una internetwork que utilice VLSM.

Resumen manual de ruta: Esta sección explica el concepto de resumen manual de ruta y describe cómo diseñar interredes que permitan un fácil resumen.

Autoresumen y redes con clases separadas: Esta sección examina la característica del autoresumen y explica cómo tenerla en cuenta en el diseño de internetworks con redes separadas o discontinuas.

CAPÍTULO 5

VLSM y resumen de rutas

Mientras el Capítulo 4, "Enrutamiento IP: rutas estáticas y conectadas", se centra en los temas de enrutamiento IP, este capítulo se centra en los temas relativos al direccionamiento IP: Máscaras de subred de longitud variable (VLSM, *variable-length subnet masking*), resumen manual de ruta, y resumen automático de ruta. Estas características relativas al direccionamiento IP requieren de un razonamiento acerca del rango de direcciones IP implicado por una dirección y máscara dadas, o por la subred que es parte de una ruta resumida. Por tanto, es necesario un completo entendimiento del direccionamiento IP para poder entender completamente los ejemplos del capítulo.

Este capítulo se centra principalmente en los conceptos y comandos show, con sólo unos pocos comandos de configuración de interés.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las ocho preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 5.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

Tabla 5.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
VLSM	1-3
Resumen manual de ruta	4-6
Autoresumen y redes con clase separadas	7-8

1. ¿Cuáles de los siguientes protocolos soportan VLSM?
   a. RIP-1
   b. RIP-2
   c. EIGRP
   d. OSPF
2. ¿Qué significan las siglas VLSM?
   a. Máscara de subred de longitud variable (*Variable-length subnet mask*).
   b. Máscara de subred muy larga (*Very long subnet mask*).
   c. Máscara de subred longitudinalmente vociferante (*Vociferous longitudinal subnet mask*).
   d. Máscara de subred por vector de longitud (*Vector-length subnet mask*).
   e. Máscara de subred de bucle vector (*Vector loop subnet mask*).
3. R1 ha configurado la interfaz Fa0/0 con el comando `ip address 10.5.48.1 255.255.240.0`. ¿Cuál de las siguientes subredes, cuando se configuren en otra interfaz de R1, podría no ser considerada una subred VLSM solapada?
   a. 10.5.0.0 255.255.240.0
   b. 10.4.0.0 255.254.0.0
   c. 10.5.32.0 255.255.224.0
   d. 10.5.0.0 255.255.128.0
4. ¿Cuál de las siguientes subredes resumidas es la ruta resumida menor (menor rango de direcciones) que incluye las subredes 10.3.95.0, 10.3.96.0 y 10.3.97.0, máscara 255.255.255.0?
   a. 10.0.0.0 255.0.0.0
   b. 10.3.0.0 255.255.0.0
   c. 10.3.64.0 255.255.192.0
   d. 10.3.64.0 255.255.224.0
5. ¿Cuál de las siguientes subredes resumidas no es un resumen válido que incluya las subredes 10.1.55.0, 10.1.56.0 y 10.1.57.0, máscara 255.255.255.0?
   a. 10.0.0.0 255.0.0.0
   b. 10.1.0.0 255.255.0.0
   c. 10.1.55.0 255.255.255.0
   d. 10.1.48.0 255.255.248.0
   e. 10.1.32.0 255.255.224.0
6. ¿Cuáles de los siguientes protocolos soportan el resumen manual de ruta?
   a. RIP-1
   b. RIP-2
   c. EIGRP
   d. OSPF

7. ¿Cuáles de los protocolos de enrutamiento soportan el autoresumen de manera predeterminada?
   a. RIP-1
   b. RIP-2
   c. EIGRP
   d. OSPF
8. Una internetwork tiene una red separada 10.0.0.0, y está teniendo problemas. Todos los routers usan RIP-1 con todas las configuraciones predeterminadas. ¿Cuál de las siguientes respuestas especifica una acción que, por sí misma, podría solucionar el problema y permitir la red separada?
   a. Migrar todos los routers a OSPF, utilizando el mayor número de valores predeterminados posibles.
   b. Deshabilitar el autoresumen con el comando de configuración de RIP `no auto-summary`.
   c. Migrar a EIGRP, utilizando el mayor número de valores predeterminados posibles.
   d. El problema no se puede resolver sin hacer primero a la red 10.0.0.0 contigua.

Temas fundamentales

Este capítulo discute tres temas relacionados: VLSM, resumen manual de ruta y resumen automático de ruta. Estos temas relacionados principalmente debido a la matemática subyacente, requieren que el ingeniero sea capaz de mirar un número de subred y máscara y rápidamente determinar el rango de direcciones implícito. Este capítulo comienza con VLSM, pasando por el resumen manual de ruta, y finalmente por el autoresumen.

VLSM

VLSM ocurre cuando una internetwork utiliza más de una máscara en diferentes subredes de una única red de Clase A, B o C. VLSM permite a los ingenieros reducir el número de direcciones IP utilizadas en cada subred, permitiendo más subredes y evitando tener que obtener otro número de red IP registrado en las autoridades regionales de asignación de direcciones IP. Incluso cuando se usan redes IP privadas (como las descritas en la RFC 1918), las grandes corporaciones podrían aún necesitar conservar el espacio de direcciones, surgiendo de nuevo la necesidad de usar VLSM.

La Figura 5.1 muestra un ejemplo de VLSM usado en la red de clase A 10.0.0.0.

La Figura 5.1 muestra una típica opción con un prefijo /30 (máscara 255.255.255.252) en enlaces serie punto a punto y con alguna otra máscara (255.255.255.0, en este ejemplo) en las

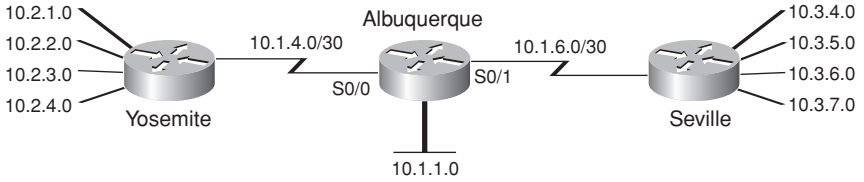


Figura 5.1. VLSM en la red 10.0.0.0: máscaras 255.255.255.0 y 255.255.255.252.

subredes LAN. Todas las subredes son de la red de clase A 10.0.0.0, con dos máscaras en uso; por tanto, coincide con la definición de VLSM.

De forma extraña, es un error común pensar que VLSM significa "usar más de una máscara", en vez de "usar más de una máscara en una única red con clase". Por ejemplo, si en un diagrama de internetwork, todas las subredes de la red 10.0.0.0 utilizan la máscara 255.255.240.0 y todas las subredes de la red 11.0.0.0 usan la máscara 255.255.255.0, se utilizan dos máscaras diferentes. Sin embargo, sólo hay una máscara en cada respectiva red con clase; por tanto, este particular diseño podría no usar VLSM.

El Ejemplo 5.1 muestra la tabla de enrutamiento de Albuquerque de la Figura 5.1 Albuquerque utiliza dos máscaras en la red 10.0.0.0, como se señala en la línea sombreada del ejemplo.

Ejemplo 5.1. Tabla de Enrutamiento de Albuquerque con VLSM.

```
Albuquerque#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
D       10.2.1.0/24 [90/2172416] via 10.1.4.2, 00:00:34, Serial0/0
D       10.2.2.0/24 [90/2172416] via 10.1.4.2, 00:00:34, Serial0/0
D       10.2.3.0/24 [90/2172416] via 10.1.4.2, 00:00:34, Serial0/0
D       10.2.4.0/24 [90/2172416] via 10.1.4.2, 00:00:34, Serial0/0
D       10.3.4.0/24 [90/2172416] via 10.1.6.2, 00:00:56, Serial0/1
D       10.3.5.0/24 [90/2172416] via 10.1.6.2, 00:00:56, Serial0/1
D       10.3.6.0/24 [90/2172416] via 10.1.6.2, 00:00:56, Serial0/1
D       10.3.7.0/24 [90/2172416] via 10.1.6.2, 00:00:56, Serial0/1
C       10.1.1.0/24 is directly connected, Ethernet0/0
C       10.1.6.0/30 is directly connected, Serial0/1
C       10.1.4.0/30 is directly connected, Serial0/0
```

Protocolos de enrutamiento sin clase y con clase

Para un protocolo de enrutamiento que soporte VLSM, el protocolo de enrutamiento debe publicar no sólo el número de subred, sino también la máscara de subred cuando publica rutas. Además, un protocolo de enrutamiento debe incluir las máscaras de subred en sus actualizaciones de enrutamiento para soportar el resumen manual de ruta.

Cada protocolo IP se considera con o sin clase basándose en si el protocolo de enrutamiento envía (sin clase) o no (con clase) la máscara en sus actualizaciones de enrutamiento. Cada protocolo de enrutamiento es sin clase o con clase por su propia naturaleza; no existen comandos para habilitar o deshabilitar si un protocolo de enrutamiento particular es un protocolo de enrutamiento sin clase o con clase. La Tabla 5.2 lista los protocolos de enrutamiento, mostrando en cada uno si es sin clase o con clase, y ofrece un recordatorio de las dos características (VLSM y resumen de ruta) habilitadas por la inclusión de máscaras en las actualizaciones de enrutamiento.

Tabla 5.2. Protocolos de enrutamiento interior de IP sin clase y con clase.

Protocolo de enrutamiento	¿Es sin clase?	Envía máscara en actualizaciones	Soporta VLSM	Soporta el resumen manual de ruta
RIP-1	No	No	No	No
IGRP	No	No	No	No
RIP-2	Sí	Sí	Sí	Sí
EIGRP	Sí	Sí	Sí	Sí
OSPF	Sí	Sí	Sí	Sí

Subredes VLSM solapadas

Las subredes elegidas para ser utilizadas en un diseño cualquiera de intenetwork IP no deben solapar sus rangos de direcciones. Con una única máscara de subred en una red, las superposicones son algo obvias; no obstante, con VLSM, el solapamiento de subredes podría no ser tan obvio. Cuando múltiples subredes se solapan, las entradas en la tabla de enrutamiento del router se solapan. Como resultado, el enrutamiento llega a ser impredecible, y algunos hosts pueden ser rechazados por sólo una parte concreta de la internetwork. En resumen, un diseño que utilice subredes solapadas es considerado un diseño incorrecto, y no debe utilizarse.

Existen dos tipos generales de problemas relativos a subredes VLSM solapadas, tanto en trabajos reales como en los exámenes: analizar un diseño existente para encontrar los

solapamientos y elegir nuevas subredes VLSM sin crear subredes solapadas. Para apreciar cómo puede el examen tratar VLSM y las subredes solapadas, considérese la Figura 5.2, que muestra una única red de Clase B (172.16.0.0), usando un diseño VLSM que incluye tres máscaras diferentes, / 23, /24 y /30.

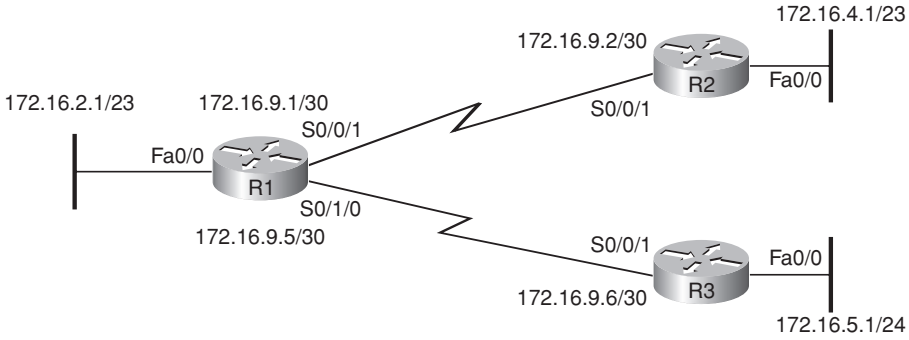


Figura 5.2. Diseño VLSM con posible solapamiento.

Imagine ahora que una pregunta del examen muestra la figura, y bien directa o indirectamente pregunta si existen subredes solapadas. Este tipo de preguntas podrían simplemente decir que algunos hosts no pueden hacer *ping* a otros, o podrían no hacer mención a que la causa raíz podría ser que algunas de las subredes se solapan. Para contestar estas preguntas, seguir esta sencilla pero posiblemente laboriosa tarea:

Paso 1 Calcular el número de subred y la dirección de difusión en cada subred; se obtendrán así los rangos de direcciones de cada subred.

Paso 2 Comparar los rangos de direcciones en cada subred y buscar los casos en los cuales los rangos se solapan.

Por ejemplo, en la Figura 5.2, se pueden ver cinco subredes, y usando el Paso 1, se calculan los números de subred, las direcciones de difusión y el rango de direcciones. Las respuestas se presentan en la Tabla 5.3.

Tabla 5.3. Subredes y rangos de direcciones de la Figura 5.2.

Localización de la subred	Número de subred	Primera dirección	Última dirección	Dirección de difusión
LAN R1	172.16.2.0	172.16.2.1	172.16.3.254	172.16.3.255
LAN R2	172.16.4.0	172.16.4.1	172.16.5.254	172.16.5.255
LAN R3	172.16.5.0	172.16.5.1	172.16.5.254	172.16.5.255
Serie R1-R2	172.16.9.0	172.16.9.1	172.16.9.2	172.16.9.3
Serie R1-R3	172.16.9.4	172.16.9.5	172.16.9.6	172.16.9.7

El Paso 2 es el paso obvio de comparar los rangos de direcciones para comprobar si existe algún solapamiento. Observe que ninguno de los números de subred son idénticos; no obstante, un examen más detallado de las subredes LAN R2 y LAN R3 muestra que se solapan. En este caso, el diseño es inválido por el solapamiento, y habría que cambiar una de las dos subredes.

Diseño de un escenario de subredes empleando VLSM

El libro *CCENT/CCNA ICND1 Guía oficial para el examen de certificación* explica cómo diseñar un escenario de direccionamiento IP para una nueva internetwork seleccionando subredes cuando se utiliza una única máscara de subred a lo largo de una red con clase. Para hacer esto, el proceso primero analiza los requisitos de diseño para determinar el número de subredes y el número de hosts en la subred más grande. Entonces, se elige una máscara de subred. Finalmente, todas las posibles subredes de la red, que utilizan esa máscara, son identificadas, y las subredes actuales utilizadas en el diseño se eligen de esa lista. Por ejemplo, en la red de Clase B 172.16.0.0, un diseño podría necesitar diez subredes, con un máximo de 200 hosts por subred. La máscara 255.255.255.0 cumple estos requisitos, con 8 bits de subred y 8 bits de host, soportando 256 subredes y 254 hosts por subred. Los números de subred podrían ser 172.16.0.0, 172.16.1.0, 172.16.2.0, y así sucesivamente.

Cuando se usa VLSM en un diseño, el proceso de diseño empieza decidiendo cuántas subredes de cada tamaño se necesitan. Por ejemplo, muchas instalaciones utilizan subredes con un prefijo /30 para enlaces serie porque estas subredes soportan exactamente dos direcciones IP, que son todas las direcciones necesarias en un enlace punto a punto. Las subredes basadas en LAN a menudo tienen diferentes requisitos, con longitudes más pequeñas del prefijo (más bits de host) para un número grande de hosts/subred, y longitudes mayores del prefijo (menos bits de host) para números más pequeños de hosts/subred.

Nota

Para revisar el diseño de subredes cuando se utilizán máscaras de subred de longitud estática (SLSM), referirse a *CCENT/CCNA ICND1 Guía oficial para el examen de certificación*, Capítulo 12. (El Apéndice D que sólo encontrará en el DVD del libro también incluye algunos problemas prácticos relacionados.)

Una vez determinado el número de subredes con cada máscara, el siguiente paso es encontrar los números de subredes que cumplan los requisitos. Esta tarea no es particularmente difícil si ya se ha entendido cómo encontrar los números de subred cuando se usan máscaras de longitud estática. Sin embargo, un proceso más formal puede ayudar, el cual se perfila como sigue:

Paso 1 Determinar el número de subredes necesarias para cada máscara/prefijo basándose en los requisitos del diseño.

Paso 2 Usando la longitud de prefijo más corta (el mayor número de bits de host), identificar las subredes de la red con clase cuando usan esa máscara, hasta que el número necesario de tales subredes haya sido identificado.

Paso 3 Identificar el número de subred numérico siguiente usando la misma máscara como en el paso anterior.

Paso 4 Comenzando con el número de subred identificado en el paso anterior, identificar subredes más pequeñas basándose en la longitud de prefijo siguiente más larga requerida por el diseño, hasta que el número necesario de subredes de ese tamaño haya sido identificado.

Paso 5 Repetir los pasos 3 y 4 hasta encontrar todas las subredes de todos los tamaños.

Francamente, usar el proceso anterior, como está escrito, puede tener cierta dificultad, pero un ejemplo puede ayudar a dar sentido a este proceso. Así, imagine un diseño de red en el que se han determinado los siguientes requisitos, que corresponde al Paso 1 del proceso previo. El diseño requiere utilizar la red de Clase B 172.16.0.0:

- Tres subredes con máscara /24 (255.255.255.0).
- Tres subredes con máscara /26 (255.255.255.192).
- Cuatro subredes con máscara /30 (255.255.255.252).

El Paso 2 en este caso significa que la primera de las tres subredes de la red 172.16.0.0 podría ser identificada, con la máscara /24, porque /24 es la longitud de prefijo más pequeña de las tres longitudes de prefijo listadas en los requisitos de diseño. Usando la misma matemática tratada en el libro ICND1, las primeras tres subredes podrían ser 172.16.0.0/24, 172.16.1.0/24 y 172.16.2.0/24:

- 172.16.0.0/24: Rango 172.16.0.1–172.16.0.254
- 172.16.1.0/24: Rango 172.16.1.1–172.16.1.254
- 172.16.2.0/24: Rango 172.16.2.1–172.16.2.254

El Paso 3 consiste en identificar una subred más con la máscara /24; por tanto, la subred numérica siguiente podría ser 172.16.3.0/24.

Antes de pasar al Paso 4, tómese unos minutos para revisar la Figura 5.3. La figura muestra el resultado del Paso 2 en la parte superior, listando las tres subredes identificadas en este paso como "asignadas" porque serán usadas por las subredes en este diseño. También muestra la siguiente subred, como se encuentra en el Paso 3, listándola como no asignada, porque aún no ha sido elegida para utilizarse en una parte concreta del diseño.

Para encontrar las subredes como indica el Paso 4, comenzar con el número de subred sin asignar encontrado en el Paso 3 (172.16.3.0), pero con el Paso 4 aplicando la longitud de prefijo siguiente más larga, o /26 en este ejemplo. El proceso siempre resulta en el primer número de subred siendo el número de subred encontrado en el paso previo, ó 172.16.3.0 en este caso. Las tres subredes son las siguientes:

- 172.16.3.0/26: Rango 172.16.3.1–172.16.3.62
- 172.16.3.64/26: Rango 172.16.3.65–172.16.3.126
- 172.16.3.128/26: Rango 172.16.3.129–172.16.3.190

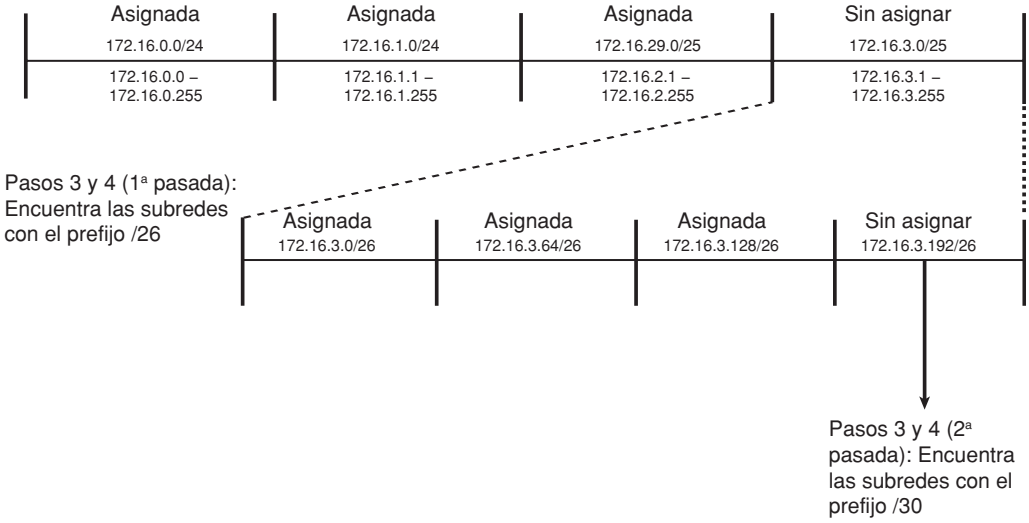


Figura 5.3. Diseñando para utilizar subredes VLSM.

Finalmente, el Paso 5 dice repetir los Pasos 3 y 4 hasta que todas las subredes se hayan encontrado. En este caso, repitiendo el Paso 3, se encuentra la siguiente subred, usando la longitud de prefijo /26; la denominada subred 172.16.3.192/26. Esta subred es considerada de momento como sin asignar. Para repetir el Paso 4 para la longitud de prefijo siguiente más larga, el Paso 4 utiliza el prefijo /30, comenzando con el número de subred 172.16.3.192. La primera subred será 172.16.3.192, con máscara /30, más las siguientes tres subredes con la misma máscara, como sigue:

- 172.16.3.192/30: Rango 172.16.3.193–172.16.3.194
- 172.16.3.196/30: Rango 172.16.3.197–172.16.3.198
- 172.16.3.200/30: Rango 172.16.3.201–172.16.3.202
- 172.16.3.204/30: Rango 172.16.3.205–172.16.3.206

La fraseología del proceso formalizado puede parecer un poco laboriosa, pero produce un conjunto de subredes que no se solapan. Asumiendo que con este planteamiento estructurado de asignar primero las subredes más grandes y después las subredes más pequeñas, normalmente se pueden elegir subredes en las que los rangos de direcciones no se solapan.

Adición de una nueva subred a un diseño existente

Otra tarea requerida cuando se trabaja con internetworks basadas en VLSM es elegir un nuevo número de subred para una internetwork existente. En particular, se debe poner espe-

cial atención cuando se eligen nuevos números de subred para evitar solapamientos entre la nueva subred y cualquiera de las subredes existentes. Por ejemplo, considerar la internetwork de la Figura 5.2, con la red con clase 172.16.0.0. Una pregunta de examen podría sugerir que hay que añadir al diseño una nueva subred con una longitud de prefijo /23. La pregunta podría también decir, "Seleccione el número menor de subred que se pueda usar para esta nueva subred". Por tanto, se deben identificar las subredes, y elegir una subred no solapada.

Para abordar este problema, se necesitará encontrar todos los números de subred que se pueden crear en esa red con clase, usando la máscara declarada o implícita. Después, hay que asegurarse de que la nueva subred no se solapa con cualquiera de las subredes existente. Específicamente, se pueden usar los siguientes pasos:

Tema clave

Paso 1 Si no se especifica como parte de la pregunta, elegir la máscara de subred (longitud del prefijo) basándose en los requisitos de diseño, normalmente basándose en el número de hosts necesarios en la subred.

Paso 2 Calcular todos los números posibles de subred de la red con clase, usando la máscara determinada en el Paso 1. (Si la pregunta del examen pregunta por el número de subred numéricamente mayor o más largo, sólo puede realizar este cálculo para las pocas primeras o últimas subredes.)

Paso 3 Para las subredes encontradas en el Paso 2, calcular la dirección de difusión de la subred y el rango de direcciones para cada subred asumida.

Paso 4 Compare las listas de las subredes potenciales y rangos de direcciones con las subredes y los rangos de direcciones existentes. Descartar cualquiera de las subredes potenciales que se solapen con la subred existente.

Paso 5 Elegir un número de subred de la lista encontrada en el Paso 2 que no se solape con las subredes existentes; observe si se pregunta por el número de subred menor o mayor.

Usando este proceso de cinco pasos con el ejemplo iniciado justo antes de la lista de pasos con la Figura 5.2, la pregunta proporciona la longitud de prefijo de /23 (Paso 1). La Tabla 5.4 muestra los resultados de los Pasos 2 y 3, listando los números de subred, muestra direcciones de difusión y el rango de direcciones para las primeras cinco de las subredes /23 posibles.

Tabla 5.4. Primeras cinco subredes /23 posibles.

Subred	Número de subred	Primera dirección	Última dirección	Dirección de difusión
Primera (cero)	172.16.0.0	172.16.0.1	172.16.1.254	172.16.1.255
Segunda	172.16.2.0	172.16.2.1	172.16.3.254	172.16.3.255
Tercera	172.16.4.0	172.16.4.1	172.16.5.254	172.16.5.255
Cuarta	172.16.6.0	172.16.6.1	172.16.7.254	172.16.7.255
Quinta	172.16.8.0	172.16.8.1	172.16.9.254	172.16.9.255

El Paso 4 compara la información de la tabla con las subredes existentes. En este caso, las subredes segunda, tercera y cuarta de la Tabla 5.4 se solapan con las subredes existentes en la Figura 5.2.

El Paso 5 tiene más que ver con el examen que con las redes reales. Las preguntas de respuesta múltiple a veces necesitan forzar la pregunta para que tenga sólo una única respuesta. Así, preguntan por la subred numéricamente menor o mayor que resuelve el problema. Este problema de ejemplo en particular pregunta el número de subred menor, y la subred cero está todavía disponible (172.16.0.0/23, con la dirección de difusión 172.16.1.255). Si la pregunta permite el uso de la subred cero, la subred cero (172.16.0.0/23) podría ser la respuesta correcta. Sin embargo, si la subred cero estuviera prohibida, la primera de las cuatro subredes listadas en la Tabla 5.4 podría no estar disponible, convirtiendo a la quinta subred (172.16.8.0/23) en la respuesta correcta. Observe que el Escenario 5 del Apéndice F que encontrará en el DVD, le da una oportunidad de practicar usando este proceso particular.

Nota

Para el examen, la subred cero debe evitarse si (a) la pregunta implica el uso de protocolos de enrutamiento con clase o (b) los routers están configurados con el comando de configuración global no ip subnetzero. En otro caso, asumir que la subred cero se puede utilizar.

Configuración de VLSM

Los routers no habilitan o deshabilitan VLSM como una característica configurable. Desde la perspectiva de configuración, VLSM es simplemente un efecto colateral del subcomando de interfaz ip address. Los routers configuran VLSM por virtud de tener al menos dos interfaces de router, en el mismo router o entre todos los de la internetwork, con direcciones IP en la misma red con clase pero con máscaras diferentes. El Ejemplo 5.2 muestra un ejemplo sencillo en el router R3 de la Figura 5.2, asignando la dirección IP 172.16.5.1/24 a la interfaz Fa0/0 y a la interfaz S0/0/1 la dirección IP 172.16.9.6/30; por tanto, se usan al menos dos máscaras diferentes en la red 172.16.0.0.

Los protocolos de enrutamiento sin clase, que soportan VLSM, no tienen que ser configurados para habilitar VLSM. El soporte de VLSM es únicamente una característica inherente a estos protocolos de enrutamiento.

Ejemplo 5.2. Configuración de VLSM.

```
R3#configure terminal
R3(config)#interface Fa0/0
R3(config-if)#ip address 172.16.5.1 255.255.255.0
R3(config-if)#interface S0/0/1
R3(config-if)#ip address 172.16.9.6 255.255.255.252
```

A continuación, el texto pasa a la segunda sección principal de este capítulo, el tema del resumen manual de ruta.

Resumen manual de ruta

Las redes pequeñas pueden tener solamente unas pocas docenas de rutas en las tablas de enrutamiento de sus routers. Cuanto más grande es la red, más grande es el número de rutas. De hecho, los routers de Internet tienen más de 100.000 rutas en algunos casos.

La tabla de enrutamiento puede llegar a ser muy grande en redes IP grandes. A medida que las tablas crecen, consumen más memoria en un router. También, cada router tarda más en enrutar un paquete, porque el router tiene que buscar la ruta en la tabla de enrutamiento, y buscar en un tabla grande generalmente lleva más tiempo. Y con una tabla de enrutamiento grande, se tarda más en solucionar un problema, porque los ingenieros que trabajan en la red necesitan examinar más información.

El **resumen de ruta** reduce el tamaño de las tablas de enrutamiento mientras mantienen las rutas a todos los destinos de la red. Como resultado, el rendimiento del enrutamiento puede mejorar y ahorrar memoria en cada router. El resumen también mejora el tiempo de convergencia, porque el router que resume las rutas no tiene que volver a publicar ningún cambio en el estado de las subredes individuales. Publicando sólo que la ruta resumida está *up* o *down*, los routers que tienen el resumen de rutas no tienen que converger cada vez que las subredes componentes pasan a *up* o *down*.

Este capítulo se refiere al resumen de ruta como resumen manual de ruta, en contraste con el último tema principal de este capítulo, el autoresumen. El término **manual** se refiere al hecho de que el resumen manual de ruta sólo ocurre cuando un ingeniero configura uno o más comandos. El autoresumen ocurre automáticamente sin ningún comando de configuración específico.

Las siguientes secciones examinan los conceptos comenzando por el resumen de ruta, seguido por algunas sugerencias sobre cómo determinar buenos resúmenes de rutas. Observe que aunque se tratan los conceptos, la configuración de rutas resumidas manualmente no se trata como un fin en sí mismo en este libro.

Conceptos de los resúmenes de ruta

Los ingenieros utilizan el resumen de ruta para reducir el tamaño de las tablas de enrutamiento en la red. El resumen de ruta causa que cierta cantidad de rutas más específicas sean reemplazadas por una única ruta que incluye todas las direcciones IP cubiertas por las subredes en las rutas originales.

Las rutas resumidas, que reemplazan múltiples rutas, deben ser configuradas por un ingeniero de redes. Aunque el comando de configuración no es exactamente como el comando `static route`, se configura la misma información básica. Ahora, el protocolo de enrutamiento publica la ruta resumida, en vez de las rutas originales.

El resumen de ruta funciona mejor si la red se diseñó con el resumen de ruta en mente. Por ejemplo, la Figura 5.1 muestra el resultado de una buena planificación para el resumen. En esta red, el ingeniero planificó sus elecciones de números de subred con el objetivo de usar el resumen de ruta. Todas las subredes del sitio principal (Albuquerque), incluyendo enlaces WAN, comienzan por 10.1. Todas las subredes LAN de Yosemite comienzan por 10.2, e igualmente, todas las subredes LAN de Seville comienzan por 10.3.

Anteriormente, el Ejemplo 5.1 mostró una copia de la tabla de enrutamiento de Albuquerque sin resumen. Este ejemplo muestra cuatro rutas de Albuquerque para subredes que comienzan por 10.2, todas apuntando su interfaz serie 0/0 a Yosemite. De forma similar, Albuquerque muestra cuatro rutas a subredes que empiezan por 10.3, todas apuntando la interfaz serie 0/1 a Seville. Este diseño permite a los routers Yosemite y Seville publicar una única ruta resumida en lugar de las cuatro rutas que publican actualmente a Albuquerque, respectivamente.

El Ejemplo 5.3 muestra el resultado de la configuración del resumen manual de ruta en Yosemite y Seville. En este caso, Yosemite está publicando una ruta resumida para 10.2.0.0/16, que representa el rango de direcciones 10.2.0.0–10.2.255.255 (todas las direcciones que comienzan por 10.2). Seville publica una ruta resumida para 10.3.0.0/16, que representa el rango de direcciones 10.3.0.0–10.3.255.255 (todas las direcciones que comienzan por 10.3).

Ejemplo 5.3. Tabla de enrutamiento de Albuquerque después del resumen de ruta.

```
Albuquerque#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D        10.2.0.0/16 [90/2172416] via 10.1.4.2, 00:05:59, Serial0/0
D        10.3.0.0/16 [90/2172416] via 10.1.6.3, 00:05:40, Serial0/1
C        10.1.1.0/24 is directly connected, Ethernet0/0
C        10.1.6.0/30 is directly connected, Serial0/1
C        10.1.4.0/30 is directly connected, Serial0/0
```

La tabla de enrutamiento de Albuquerque enruta todavía los paquetes correctamente, pero más eficientemente y con menor memoria. Francamente, mejorar de 11 a 5 rutas no ayuda demasiado, pero el mismo concepto, aplicado a grandes redes, sí puede ser significativo.

Los efectos del resumen de ruta pueden verse también en los otros dos routers de la figura. El Ejemplo 5.4 muestra Yosemite, incluyendo la configuración del resumen de ruta y la tabla de enrutamiento de Yosemite. El Ejemplo 5.5 muestra el mismo tipo de información en Seville.

Ejemplo 5.4. Configuración de Yosemite y la tabla de enrutamiento después del resumen de ruta.

```
Yosemite#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yosemite(config)#interface serial 0/0
Yosemite(config-if)#ip summary-address eigrp 1 10.2.0.0 255.255.0.0
Yosemite(config-if)#^Z

Yosemite#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
D       10.2.0.0/16 is a summary, 00:04:57, Null0
D       10.3.0.0/16 [90/2684416] via 10.1.4.1, 00:04:30, Serial0/0
C       10.2.1.0/24 is directly connected, FastEthernet0/0
D       10.1.1.0/24 [90/2195456] via 10.1.4.1, 00:04:52, Serial0/0
C       10.2.2.0/24 is directly connected, Loopback2
C       10.2.3.0/24 is directly connected, Loopback3
C       10.2.4.0/24 is directly connected, Loopback4
D       10.1.6.0/30 [90/2681856] via 10.1.4.1, 00:04:53, Serial0/0
C       10.1.4.0/30 is directly connected, Serial0/0
```

Ejemplo 5.5. Configuración de Seville y la tabla de enrutamiento después del resumen de ruta.

```
Seville#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Seville(config)#interface serial 0/0
Seville(config-if)#ip summary-address eigrp 1 10.3.0.0 255.255.0.0
Seville(config-if)#^Z
Seville#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

(continúa)

Ejemplo 5.5. Configuración de Seville y la tabla de enrutamiento después del resumen de ruta *(continuación)*.

```
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
D       10.2.0.0/16 [90/2684416] via 10.1.6.1, 00:00:36, Serial0/0
D       10.3.0.0/16 is a summary, 00:00:38, Null0
D       10.1.1.0/24 [90/2195456] via 10.1.6.1, 00:00:36, Serial0/0
C       10.3.5.0/24 is directly connected, Loopback5
C       10.3.4.0/24 is directly connected, FastEthernet0/0
C       10.1.6.0/30 is directly connected, Serial0/0
C       10.3.7.0/24 is directly connected, Loopback7
D       10.1.4.0/30 [90/2681856] via 10.1.6.1, 00:00:36, Serial0/0
C       10.3.6.0/24 is directly connected, Loopback6
```

La configuración del resumen de ruta varía con los diferentes protocolos de enrutamiento; en este ejemplo se usa IGRP mejorado (EIGRP). Las rutas resumidas para EIGRP se crean con el subcomando de interfaz ip summary-address en Yosemite y Seville en este caso. Cada comando define una nueva ruta resumida y le dice a EIGRP que sólo publique el resumen por esta interfaz y no publique ninguna otra ruta contenida en el resumen mayor. Por ejemplo, Yosemite define una ruta resumida de 10.2.0.0, máscara 255.255.0.0, que define una ruta para todos los hosts cuya dirección IP comience con 10.2. En efecto, este comando causa que Yosemite y Seville publiquen las rutas 10.2.0.0 255.255.0.0 y 10.3.0.0 255.255.0.0, respectivamente, y no publiquen sus cuatro subredes LAN originales.

Observe que antes en el Ejemplo 5.3, la tabla de enrutamiento de Albuquerque contiene ahora una ruta a 10.2.0.0 255.255.0.0 (la máscara se muestra en la notación de prefijo como /16), pero ninguna de las cuatro subredes originales que empiezan por 10.2. Lo mismo ocurre para la ruta 10.3.0.0/16.

Las tablas de enrutamiento de Yosemite y Seville parecen un poco diferentes a Albuquerque. Centrándonos en Yosemite (Ejemplo 5.4), observe que las cuatro rutas de subredes que empiezan por 10.2 aparecen *up* porque son subredes directamente conectadas. Yosemite no ve las cuatro rutas 10.3. En cambio, ve una ruta resumida, porque Albuquerque ahora publica solamente la ruta resumida 10.3.0.0/16. Lo opuesto es cierto en Seville (Ejemplo 5.5), que lista todas las cuatro rutas conectadas que comienzan con 10.3 y una ruta resumida para 10.2.0.0/16.

La parte más interesante de las tablas de enrutamiento de Yosemite es la ruta a 10.2.0.0/16, con la interfaz de salida establecida a null0. Las rutas referenciadas como una interfaz de salida de interfaz null0 significan que los paquetes que coincidan con esta ruta son descartados. EIGRP añade esta ruta, con la interfaz null0, como resultado del comando ip summary-address. La lógica funciona como sigue:

Yosemite necesita esta ruta de aspecto extraño porque ahora podría recibir paquetes destinados a otras direcciones 10.2 además de las cuatro subredes 10.2 existentes. Si llega un paquete destinado a una de las cuatro subredes 10.2.x existentes, Yosemite tiene una ruta correcta, más específica que coincide con la del paquete. Si llega un paquete cuyo destino comienza por 10.2, pero no es de ninguna de estas cuatro subredes, la ruta nula (*null*) coincide con la del paquete, causando que Yosemite descarte el paquete (como debe hacer).

La tabla de enrutamiento de Seville es similar a la de Yosemite en cuanto a las entradas de la tabla y en el porqué se encuentran en la tabla.

Estrategias de los resúmenes de rutas

Como se ha mencionado antes, el resumen manual de ruta funciona mejor cuando el ingeniero de redes planifica su selección del número de subredes anticipando el resumen de ruta. Por ejemplo, los ejemplos anteriores asumen un plan bien pensado, donde los ingenieros sólo utilizan subredes que empiezan por 10.2 para las subredes del router Yosemite. Esta convención permite la creación de una ruta resumida para todas las direcciones que empiezan por 10.2 haciendo que Yosemite publique una ruta describiendo la subred 10.2.0.0, máscara 255.255.0.0.

Algunas rutas resumidas combinan varias rutas en una, pero podrían no ser el "mejor" resumen. La palabra "mejor", cuando se aplica a la selección de qué ruta resumen configurar, significa que el resumen podría incluir todas las subredes especificadas en la pregunta pero con las menos direcciones posibles. Por ejemplo, en el ejemplo anterior de resumen, Yosemite resume cuatro subredes (10.2.1.0, 10.2.2.0, 10.2.3.0 y 10.2.4.0, todas con la máscara 255.255.255.0) en la ruta resumida 10.2.0.0/16. Sin embargo, este resumen incluye muchas direcciones IP que no están en estas cuatro subredes. ¿Funciona el resumen dados los objetivos de diseño de la red? Seguro. Sin embargo, en lugar de definir únicamente un resumen que abarca muchas de las direcciones adicionales que aún no existen en una red, el ingeniero en cambio desea configurar el más firme, o más conciso, o mejor resumen: el resumen que incluye todas las subredes pero las menos subredes extra (aquellas que no han sido asignadas todavía) como sea posible. Esta sección describe una estrategia para encontrar estas rutas resumidas mejores y más concisas.

La siguiente lista describe un proceso binario generalizado para encontrar la mejor ruta resumida para un grupo de subredes:

Paso 1 Listar en binario todos los números de subredes a resumir.

Paso 2 Encontrar los primeros N bits de los números de subred para los cuales toda subred tiene el mismo valor, moviéndose de izquierda a derecha. (Para nuestro propósito, considerar esta primera parte la parte "en común".)

Paso 3 Para encontrar el número de subred de la ruta resumida, escribir los bits en común del Paso 2 y ceros binarios para el resto de bits. Convertir a decimal, 8 bits de cada vez, cuando se finalice.

Paso 4 Para encontrar la máscara de subred de la ruta resumida, escribir N unos binarios, siendo N el número de bits en común encontrados en el Paso 2. Comple-

tar la máscara de subred con ceros binarios. Cuando acabe, convertir a decimal, 8 bits de cada vez.

Paso 5 Verificar el trabajo calculando el rango de direcciones IP válidas implicado por la nueva ruta resumida, comparando el rango de las subredes resumidas. El nuevo resumen debería abarcar todas las direcciones IP de las subredes resumidas.

Viendo los números de subred en binario, es más fácil descubrir los bits en común de todos los números de subred. Asumiendo el número más largo de bits en común, se puede encontrar el mejor resumen. Las dos secciones siguientes muestran dos ejemplos usando este proceso para encontrar las rutas resumidas mejores, más concisas y más firmes para la red mostrada en la Figura 5.1.

Ejemplo del "mejor" resumen en Seville

Seville tiene las subredes 10.3.4.0, 10.3.5.0, 10.3.6.0 y 10.3.7.0, todas con la máscara 255.255.255.0. Comenzar el proceso escribiendo todos los números de subred en binario:

```
0000 1010 0000 0011 0000 01|00 0000 0000 - 10.3.4.0
0000 1010 0000 0011 0000 01|01 0000 0000 - 10.3.5.0
0000 1010 0000 0011 0000 01|10 0000 0000 - 10.3.6.0
0000 1010 0000 0011 0000 01|11 0000 0000 - 10.3.7.0
```

El Paso 2 requiere encontrar todos los bits en común al comienzo de todas las subredes. Incluso antes de mirar los números en binario, puede suponer que los dos primeros octetos son idénticos para las cuatro subredes. Por tanto, un rápido vistazo a los primeros 16 bits de todos los números de subred confirma que todos tienen el mismo valor. Esto significa que la parte común (Paso 2) es al menos de 16 bits de longitud. Un examen más exhaustivo muestra que los primeros 6 bits del tercer octeto son también idénticos, pero el bit séptimo del tercer octeto tiene valores diferentes para las diferentes subredes. Así la parte común de estas cuatro subredes es los 22 primeros bits.

El Paso 3 dice crear un número de subred para el resumen tomando los mismos bits en la parte común y escribiendo ceros binarios para el resto. En este caso:

```
0000 1010 0000 0011 0000 01|00 0000 0000 - 10.3.4.0
```

El Paso 4 crea la máscara usando unos binarios para los mismos bits de la parte común, que en este caso son los primeros 22 bits, y después ceros binarios para el resto de bits, como sigue:

```
1111 1111 1111 1111 1111 11|00 0000 0000 - 255.255.252.0
```

Por tanto, la ruta resumida usa la subred 10.3.4.0, máscara 255.255.252.0.

El Paso 5 sugiere un método para validar su trabajo. La ruta resumen debería incluir todas las direcciones IP de las rutas resumidas. En este caso, el rango de direcciones de

la ruta resumen comienza con 10.3.4.0. La primera dirección IP válida es 10.3.4.1, la dirección IP final es 10.3.7.254, y la dirección de difusión es 10.3.7.255. En este caso, la ruta resumen incluye todas las direcciones IP de las cuatro rutas que resume y no direcciones IP extrañas.

Ejemplo del "mejor" resumen en Yosemite

Las cuatro subredes de Yosemite no pueden resumirse tan eficientemente como las de Seville. En Seville, la ruta resumen en sí misma incluye el mismo conjunto de direcciones IP de las cuatro subredes sin direcciones extra. Como podrá ver, la mejor ruta resumida de Yosemite incluye dos veces en el resumen tantas direcciones como existen en las cuatro subredes originales.

Yosemite tiene las subredes 10.2.1.0, 10.2.2.0, 10.2.3.0 y 10.2.4.0, todas con la máscara 255.255.255.0. El proceso comienza en el Paso 1 escribiendo todos los números de subred en binario:

```
0000 1010 0000 0010 0000 0|001 0000 0000 - 10.2.1.0
0000 1010 0000 0010 0000 0|010 0000 0000 - 10.2.2.0
0000 1010 0000 0010 0000 0|011 0000 0000 - 10.2.3.0
0000 1010 0000 0010 0000 0|100 0000 0000 - 10.2.4.0
```

En el Paso 2 vemos que los dos primeros octetos son idénticos en las cuatro subredes, más los primeros 5 bits del tercer octeto. Por tanto, los primeros 21 bits de los cuatro números de subred son comunes.

El Paso 3 dice crear un número de subred para la ruta resumida tomando el mismo valor de la parte común y rellenando el resto con ceros binarios. En este caso:

```
0000 1010 0000 0010 0000 0|000 0000 0000 - 10.2.0.0
```

El Paso 4 crea la máscara usada para la ruta resumida usando unos binarios para la parte común y ceros binarios para el resto. La parte común en este ejemplo son los primeros 21 bits:

```
1111 1111 1111 1111 1111 11|00 0000 0000 - 255.255.252.0
```

Por tanto, el mejor resumen es 10.2.0.0, máscara 255.255.248.0.

El Paso 5 sugiere un método para verificar el trabajo. La ruta resumida debe definir un superconjunto de direcciones IP de las rutas resumidas. En este caso, el rango de direcciones empieza con 10.2.0.0. La primera dirección IP válida es 10.2.0.1, la dirección IP final válida es 10.2.7.254, y la dirección de difusión es 10.2.7.255. En este caso, la ruta resumida resume un conjunto más grande de direcciones que únicamente las cuatro subredes, pero incluye todas las direcciones de las cuatro subredes.

Autoresumen y redes con clase separadas

Como se ha tratado en las secciones previas, el resumen manual de ruta puede mejorar la eficiencia del enrutamiento, deducir el consumo de memoria y mejorar la convergencia reduciendo la longitud de las tablas de enrutamiento. Las secciones finales de este capítulo examinan el resumen automático de rutas en los límites de las redes con clase, utilizando una característica llamada autoresumen.

Ya que los protocolos de enrutamiento con clase no publican la información de la máscara de subred, las actualizaciones de enrutamiento simplemente listan números de subred pero no acompañados de la máscara. Un router que recibe una actualización de enrutamiento con un protocolo de enrutamiento con clase mira en el número de subred que figura en la actualización, pero el router debe deducir cuál es la máscara asociada a esa subred. Por ejemplo, con los routers de Cisco, si R1 y R2 tienen que conectar redes de una misma y única red de Clase A, B o C, y si R2 recibe una actualización de R1, R2 asume que las rutas descritas en la actualización de R1 utilizan la misma máscara que R2. Dicho de otra forma, los protocolos de enrutamiento con clase requieren una máscara de subred de longitud estática (SLSM) a lo largo de cada red con clase; así, cada router puede entonces deducir razonablemente que la máscara configurada para sus propias interfaces es la misma máscara utilizada a lo largo de toda la red con clase.

Cuando un router tiene interfaces de más de una red de Clase A, B o C, puede publicar una única ruta para una red entera de Clase A, B o C en la otra red con clase. Esta característica se llama **autoresumen**. Se caracteriza por lo siguiente:

Tema clave

> Cuando se publica por una interfaz cuya dirección IP no está en la red X, las rutas relativas a las subredes en la red X se resumen y se publican como una ruta. Esta ruta es para toda la red X de Clase A, B o C.

Dicho de otra forma, si R3 tiene interfaces en las redes 10.0.0.0 y 11.0.0.0, cuando R3 publique actualizaciones de enrutamiento por interfaces con direcciones IP que empiecen por 11, las actualizaciones publicarán una única ruta para la red 10.0.0.0. De forma similar, R3 publica una única ruta a 11.0.0.0 por sus interfaces cuya dirección IP empieza por 10.

Un ejemplo de autoresumen

Como de costumbre, un ejemplo aclara los conceptos. Considerar la Figura 5.4, que muestra dos redes en uso: 10.0.0.0 y 172.16.0.0. Seville tiene cuatro rutas (conectadas) a subredes de la red 10.0.0.0. El Ejemplo 5.6 muestra la salida del comando `show ip route` en Albuquerque, así como la salida del comando de RIP-1 `debug ip rip`.

Como muestra el Ejemplo 5.6, Albuquerque ha recibido una actualización por Serial0/1 desde Seville publicando sólo la red entera de Clase A 10.0.0.0 porque el autoresumen (de forma predeterminada) está habilitado en Seville. Como resultado, la tabla de enrutamiento IP de Albuquerque muestra únicamente una ruta a la red 10.0.0.0.

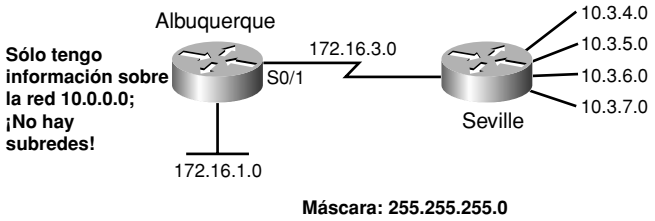


Figura 5.4. Autoresumen.

Ejemplo 5.6. Rutas de Albuquerque y depuraciones RIP.

```
Albuquerque#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, Ethernet0/0
C       172.16.3.0 is directly connected, Serial0/1
R       10.0.0.0/8 [120/1] via 172.16.3.3, 00:00:28, Serial0/1

Albuquerque#debug ip rip
RIP protocol debugging is on

00:05:36: RIP: received v1 update from 172.16.3.3 on Serial0/1
00:05:36:      10.0.0.0 in 1 hops
```

Este ejemplo también señala otra característica de cómo los protocolos de enrutamiento con clase asumen ciertos hechos. Albuquerque no tiene ninguna interfaz en la red 10.0.0.0. Así, cuando Albuquerque recibe la actualización de enrutamiento, asume que la máscara utilizada con 10.0.0.0 es 255.0.0.0, la máscara predeterminada para una red de Clase A. Dicho de otra forma, los protocolos de enrutamiento con clase esperan que el autoresumen se produzca.

Redes con clase separadas

El autoresumen no causa ningún problema con tal de que la red resumida sea contigua y no discontinua o separada. Los residentes en EE.UU. pueden apreciar el concepto de red

separada basándose en el término común **contiguo 48**, que se refiere a los 48 estados de E.E.U.U. excepto Alaska y Hawaii. Para conducir hasta Alaska desde el contiguo 48, por ejemplo, se debe conducir a través de otro país (Canadá, ¡por imposición geográfica!); por tanto, Alaska no es contigua a los 48 estados. Dicho de otra forma, está separada.

Para entender mejor el significado de los términos *contiguo y separado* en redes, refiérase a las dos definiciones formales siguientes al repasar el ejemplo de una red con clase que sigue:

- **Red contigua.** Una red con clase en la cual los paquetes que se envían entre cualquier par de subredes sólo atraviesan subredes de la misma red con clase, sin tener que pasar a través de subredes de cualquier otra red con clase.
- **Red separada.** Una red con clase en la cual los paquetes que se envían entre al menos un par de subredes deben pasar a través de subredes de una red con clase diferente.

La Figura 5.5 muestra un ejemplo de una red separada 10.0.0.0. En este caso, los paquetes que se envían desde las subredes de la red 10.0.0.0 de la izquierda, cerca de Yosemite, a las subredes de la red 10.0.0.0 de la derecha, cerca de Seville, tienen que pasar a través de las subredes de la red 172.16.0.0.

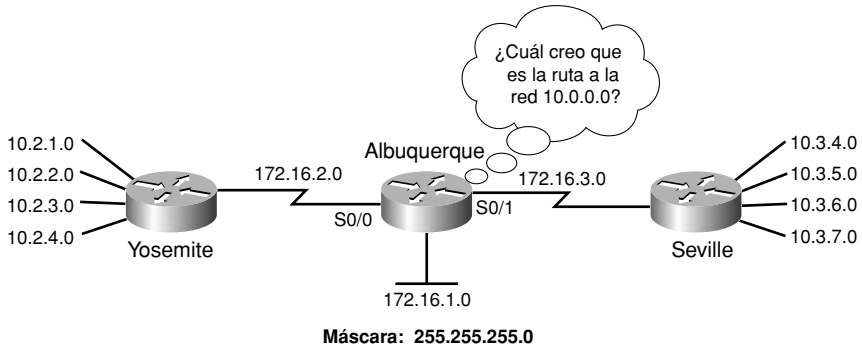


Figura 5.5. Red separada 10.0.0.0.

El autoresumen impide a una internetwork con una red separada trabajar correctamente. El Ejemplo 5.7 muestra el resultado de usar el autoresumen en la internetwork mostrada en la Figura 5.5, en este caso usando el protocolo de enrutamiento con clase RIP-1.

Como se muestra en el Ejemplo 5.7, Albuquerque ahora tiene dos rutas a la red 10.0.0.0/8: una apunta a la izquierda hacia Yosemite y otra a la derecha hacia Seville. ¡En lugar de enviar los paquetes destinados a las subredes de Yosemite por la salida Serie 0/0, Albuquerque envía algunos paquetes por S0/1 a Seville! Albuquerque simplemente equilibra los paquetes entre las dos rutas, porque hasta donde Albuquerque puede decir, las dos rutas son simplemente rutas de igual coste al mismo destino: la red 10.0.0.0 entera. Así que, las aplicaciones dejarían de funcionar correctamente en esta red.

Ejemplo 5.7. Tabla de enrutamiento de Albuquerque: el autoresumen causa problemas de enrutamiento con la red separada 10.0.0.0.

```
Albuquerque#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, Ethernet0/0
C       172.16.2.0 is directly connected, Serial0/0
C       172.16.3.0 is directly connected, Serial0/1
R       10.0.0.0/8 [120/1] via 172.16.3.3, 00:00:13, Serial0/1
                   [120/1] via 172.16.2.2, 00:00:04, Serial0/0
```

La solución a este problema es deshabilitar el uso del autoresumen. Ya que los protocolos de enrutamiento con clase deben usar el autoresumen, la solución requiere la migración a un protocolo de enrutamiento sin clase y deshabilitar la característica del autoresumen. El Ejemplo 5.8 muestra la misma internetwork que la Figura 5.5 y el Ejemplo 5.7, pero esta vez con EIGRP (sin clase), con el autoresumen deshabilitado.

Ejemplo 5.8. El protocolo de enrutamiento sin clase sin autoresumen permite redes separadas.

```
Albuquerque#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, Ethernet0/0
C       172.16.2.0 is directly connected, Serial0/0
C       172.16.3.0 is directly connected, Serial0/1
     10.0.0.0/24 is subnetted, 8 subnets
D       10.2.1.0/24 [90/2172416] via 172.16.2.2, 00:00:01, Serial0/0
D       10.2.2.0/24 [90/2297856] via 172.16.2.2, 00:00:01, Serial0/0
```

(continúa)

Ejemplo 5.8. El protocolo de enrutamiento sin clase sin autoresumen permite redes separadas *(continuación).*

```
D       10.2.3.0/24 [90/2297856] via 172.16.2.2, 00:00:01, Serial0/0
D       10.2.4.0/24 [90/2297856] via 172.16.2.2, 00:00:01, Serial0/0
D       10.3.5.0/24 [90/2297856] via 172.16.3.3, 00:00:29, Serial0/1
D       10.3.4.0/24 [90/2172416] via 172.16.3.3, 00:00:29, Serial0/1
D       10.3.7.0/24 [90/2297856] via 172.16.3.3, 00:00:29, Serial0/1
D       10.3.6.0/24 [90/2297856] via 172.16.3.3, 00:00:29, Serial0/1
```

Con el autoresumen deshabilitado en ambos, Yosemite y Seville, ninguno de los routers publica un resumen automático de la red 10.0.0.0/8 a Albuquerque. En cambio, cada router publica las subredes conocidas; así, ahora Albuquerque conoce las cuatro subredes LAN de Yosemite, así como las cuatro subredes LAN de Seville.

Soporte del autoresumen y configuración

Los protocolos de enrutamiento con clase deben usar el autoresumen. Algunos protocolos de enrutamiento sin clase soportan el autoresumen, de manera predeterminada, pero con la posibilidad de deshabilitarlo con el subcomando de router no autosummary. Otros protocolos de enrutamiento sin clase, en especial OSPF (Primero la ruta libre más corta, *Open Shortest Path First*), simplemente no soportan el autoresumen. La Tabla 5.5 resume los hechos acerca del autoresumen en los routers de Cisco.

Tabla 5.5. Soporte y valores predeterminados del autoresumen.

Protocolo de enrutamiento	¿Sin clase?	¿Soporta el autoresumen?	¿Utiliza de forma predeterminada el autoresumen?[1]	¿Puede deshabilitar el autoresumen?
RIP-1	No	Sí	Sí	No
RIP-2	Sí	Sí	Sí	Sí
EIGRP	Sí	Sí	Sí	Sí
OSPF	Sí	No	—	—

[1] Válido para las versiones principales del IOS 12.4.

También observe que la característica de autoresumen incide en los routers que conectan directamente con partes de más de una red con clase, pero no tiene impacto en routers cuyas interfaces conectan todas a una misma y única red con clase. Por ejemplo, en la Figura 5.5, la solución (como muestra el Ejemplo 5.8) requiere el subcomando de EIGRP no auto-summary en ambos, Yosemite y Seville. Sin embargo, Albuquerque, cuyas interfaces están todas en una única red (red de Clase B 172.16.0.0), podría, en este caso, no cambiar su comportamiento ni con el comando auto-summary ni con no auto-summary.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 5.6 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 5.6. Temas clave del Capítulo 5.

Tema clave	Descripción	Número de página
Tabla 5.2	Lista de los protocolos de enrutamiento IP, con hechos acerca de sin clase/con clase, soporte VLSM y soporte de resúmenes.	201
Lista	Estrategia de dos pasos para encontrar subredes VLSM solapadas.	202
Lista	Estrategia de cinco pasos para elegir una nueva subred VLSM no solapada.	206
Lista	Proceso en cinco pasos para encontrar la mejor ruta resumida manual.	212-213
Definición	Definición generalizada de autoresumen.	215
Definición	Definiciones de red contigua y red separada.	217
Tabla 5.5	Lista de protocolos de enrutamiento y hechos relativos al autoresumen.	219

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD) o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas ya completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe sus respuestas en el glosario:

Autoresumen, máscara de subred de longitud variable, protocolo de enrutamiento con clase, protocolo de enrutamiento sin clase, red con clase, red contigua, red separada, resumen de ruta, subredes solapadas.

Lectura de los escenarios del Apéndice F

El Apéndice F, "Escenarios adicionales", contiene cinco escenarios detallados que le ofrecen la oportunidad de analizar diferentes diseños, problemas y salidas de comandos y muestran conceptos interrelacionados de varios capítulos. El Escenario 1, Parte A, y todo el Escenario 5 del Apéndice F proporcionan una oportunidad de practicar y de desarrollar habilidades con VLSM.

Referencia de comandos

Este capítulo introduce sólo un nuevo comando que todavía no se había explicado en este libro, el comando del modo de configuración de router `[no] auto-summary`. Este comando habilita el autoresumen (omitiendo la opción `no`) o deshabilita el autoresumen (usando la opción `no`).

Este capítulo incluye esta sección de referencia de comandos sólo como un recordatorio del único comando a recordar de este capítulo.

Este capítulo trata los siguientes temas:

Listas de control de acceso IP estándares: Esta sección explica cómo funcionan las ACLs IP estándar y cómo se configuran.

Listas de control de acceso IP extendidas: Esta sección examina las ACLs IP más complejas, extendidas, incluyendo cómo configurarlas.

Avances en la gestión de la configuración de las ACLs: Esta sección examina los matices de dos importantes mejoras en la configuración de la ACLs durante los años: ACLs con nombre y números de secuencia.

Temas varios sobre las ACLs: Esta sección explica algunos conceptos adicionales sobre las ACLs.

CAPÍTULO 6

Listas de control de acceso IP

La seguridad de la red es uno de los temas más candentes en las redes actuales. Aunque la seguridad siempre ha sido importante, la explosión del tamaño y el alcance de Internet han creado más exposiciones de seguridad. En los pasados años, la mayoría de las compañías no estaban permanentemente conectadas a la red global (una red a través de la cual otros podrían intentar accesos ilegales a sus redes). Hoy, debido a que la mayoría de las compañías están conectadas a Internet, muchas reciben significativas entradas a través de sus servicios basados en red, hecho que incrementa la exposición e incrementa el impacto cuando la seguridad se rompe.

Los routers de Cisco pueden utilizarse como parte de una buena estrategia conjunta de seguridad. Una de las herramientas más importantes en el software IOS de Cisco, usada como parte de esta estrategia, son las listas de control de acceso (ACL). Las ACLs definen las reglas que pueden prevenir el tráfico de algunos paquetes a través de la red. Si simplemente se quiere restringir el acceso al servidor de nóminas sólo a las personas del departamento de nóminas, o si se desea evitar que los piratas de Internet lleguen hasta nuestro servidor web de comercio electrónico, las ACLs IOS pueden ser una utilidad de seguridad clave que es parte de una estrategia de seguridad mayor.

Este capítulo está en la parte II de este libro, que está orientada a los temas de enrutamiento IP. La razón de que esté en la Parte II es que el uso más típico de las ACLs en los exámenes CCNA es para el filtrado de paquetes. Así, mientras los Capítulos 4 y 5 tratan varias características que influyen en el proceso de enrutamiento IP para permitir el flujo de paquetes, este capítulo examina las ACLs que previenen el flujo de ciertos paquetes.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las diez preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 6.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al

material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

Tabla 6.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
Listas de control de acceso IP estándares	1-3
Listas de control de acceso IP extendidas	4-6
Avances en la gestión de la configuración de las ACLs	7 y 8
Temas varios sobre las ACLs	9 y 10

1. Barney es un host con la dirección IP 10.1.1.1 en la subred 10.1.1.0/24. ¿Cuáles de las siguientes son cosas que una ACL IP estándar podría hacer?
   - **a.** Correspondencia con la dirección IP de origen exacta.
   - **b.** Hacer coincidir las direcciones IP desde 10.1.1.1 hasta 10.1.1.4 con un comando access-list sin coincidencia con otras direcciones IP.
   - **c.** Hacer coincidir todas las direcciones IP en la subred de Barney con un comando access-list sin coincidencia con otras direcciones IP.
   - **d.** Correspondencia sólo con la dirección IP de destino del paquete.
2. ¿Cuál de las siguientes máscaras *wildcard* es la más útil para hacer corresponder todos los paquetes IP en la subred 10.1.128.0, máscara 255.255.255.0?
   - **a.** 0.0.0.0
   - **b.** 0.0.0.31
   - **c.** 0.0.0.240
   - **d.** 0.0.0.255
   - **e.** 0.0.15.0
   - **f.** 0.0.248.255
3. ¿Cuál de las siguientes máscaras *wildcard* es la más útil para hacer corresponder todos los paquetes IP en la subred 10.1.128.0, máscara 255.255.240.0?
   - **a.** 0.0.0.0
   - **b.** 0.0.0.31
   - **c.** 0.0.0.240
   - **d.** 0.0.0.255
   - **e.** 0.0.15.255
   - **f.** 0.0.248.255

4. ¿Cuál de los siguientes campos no puede ser comparado basándose en una ACL IP extendida?
   - **d.** Protocolo.
   - **b.** Dirección IP de origen.
   - **c.** Dirección IP de destino.
   - **d.** Byte TOS.
   - **e.** URL.
   - **f.** Nombre del fichero en las transferencias FTP.
5. ¿Cuál de los siguientes comandos access-list permite tráfico de paquetes procedentes de 10.1.1.1 a todos los servidores web cuyas direcciones IP comienzan por 172.16.5?
   - **a.** access-list 101 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
   - **b.** access-list 1951 permit ip host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
   - **c.** access-list 2523 permit ip host 10.1.1.1 eq www 172.16.5.0 0.0.0.255
   - **d.** access-list 2523 permit tcp host 10.1.1.1 eq www 172.16.5.0 0.0.0.255
   - **e.** access-list 2523 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
6. ¿Cuál de los siguientes comandos access-list permite tráfico de paquetes hacia cualquier cliente web desde todos los servidores web cuyas direcciones IP comienzan con 172.16.5?
   - **a.** access-list 101 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
   - **b.** access-list 1951 permit ip host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
   - **c.** access-list 2523 permit tcp any eq www 172.16.5.0 0.0.0.255
   - **d.** access-list 2523 permit tcp 172.16.5.0 0.0.0.255 eq www 172.16.5.0 0.0.0.255
   - **e.** access-list 2523 permit tcp 172.16.5.0 0.0.0.255 eq www any
7. ¿Cuál de los siguientes campos puede compararse utilizando una ACL IP extendida con nombre pero no con una ACL IP extendida numerada?
   - **a.** Protocolo.
   - **b.** Dirección IP de origen.
   - **c.** Dirección IP de destino.
   - **d.** Byte TOS.
   - **e.** Ninguna de las otras respuestas es correcta.
8. En un router con el IOS 12.3, un ingeniero necesita borrar la segunda línea de la ACL 101, que tiene actualmente cuatro comandos configurados. ¿Cuál de las siguientes opciones se puede usar?
   - **a.** Borrar la ACL entera y reconfigurar las tres sentencias de la ACL que deban permanecer en la misma.
   - **b.** Borrar una línea de la ACL utilizando el comando no access-list....

c. Borrar una línea de la ACL entrando en el modo de configuración de ACL para la ACL en cuestión y borrar sólo la segunda línea basándose en su número de secuencia.

d. Borrar las últimas tres líneas de la ACL desde el modo de configuración de ACL, y después volver a añadir las dos últimas sentencias a la ACL.

9. ¿Qué pauta general se podría seguir cuando se colocan las ACLs IP extendidas?

a. Realizar todo el filtrado tan cerca de la salida como sea posible.

b. Colocar primero en la ACL las sentencias más generales.

c. Filtrar los paquetes tan cerca del origen como sea posible.

d. Ordenar los comandos ACL basándose en las direcciones IP de origen, de menor a mayor, para mejorar el rendimiento.

10. ¿Cuál de las siguientes herramientas necesita el usuario general para conectar con telnet a un router para poder acceder a los hosts situados al otro lado del router?

a. ACLs con nombre.

b. ACLs reflexivas.

c. ACLs dinámicas.

d. ACLs basadas en el tiempo.

Temas fundamentales

El IOS de Cisco ha soportado las ACLs IP desde los primeros routers comerciales de Cisco a finales de los 80. El IOS identificaba estas ACLs con un número. Años después, como parte del IOS 11.2, Cisco añade la función de crear ACLs con nombre. Estas ACLs con nombre proporcionan algunos otros beneficios menores en comparación con las ACLs numeradas, pero ambas se pueden utilizar para filtrar exactamente los mismos paquetes con exactamente las mismas reglas. Finalmente, con la introducción del IOS 12.3, Cisco mejora de nuevo el soporte de ACL, en concreto en cómo el IOS permite a los ingenieros editar las ACLs existentes. Este último importante paso en la evolución de las ACLs hace que las ACLs numeradas y con nombre soporten las mismas características, excepto la diferencia obvia de utilizar unas un número y otras un nombre para identificar la ACL.

A pesar de la progresión histórica del soporte de las ACLs de Cisco, los exámenes CCNA todavía tratan gran cantidad de la misma información y comandos de configuración que han sido utilizados en los routers de Cisco al menos durante 20 años. Para soportar toda esta historia, este capítulo explica sobre todo las ACLs IP (ACLs IP numeradas) usando los mismos comandos y sintaxis disponible en el IOS durante mucho tiempo. En particular, este capítulo comienza con una descripción de los tipos de ACLs IP numeradas más sencillos (ACLs IP estándares). La segunda sección principal examina las más complejas ACLs IP extendidas, que pueden utilizase para examinar muchos de los campos de un paquete IP. A continuación de esto, la siguiente sección del capítulo describe más profun-

damente el soporte de las ACLs en el IOS; tanto la introducción del soporte de las ACLs con nombre del IOS versión 11.2, como el posterior añadido del soporte de las ACLs numeradas en secuencia y la edición mejorada de las ACL con el IOS 12.3. El capítulo finaliza abordando diversos temas relacionados con las ACLs.

Listas de control de acceso IP estándar

Las ACLs IP provocan que un router descarte algunos paquetes basándose en criterios definidos por el ingeniero de redes. El objetivo de estos filtros es evitar tráfico no deseado en la red; bien impidiendo que los piratas entren en la red o simplemente evitando que los empleados utilicen sistemas que no deben. Las listas de acceso pueden ser simplemente parte de la política de seguridad de la organización.

Por cierto, las listas de acceso IP también pueden utilizarse para filtrar actualizaciones de enrutamiento, para hacer coincidir paquetes para priorizarlos, para hacer coincidir paquetes para el *tunneling* VPN, y para hacer coincidir paquetes para implementar características de calidad de servicio. También se pueden ver las ACLs como parte de la configuración de la Conversión de direcciones de red (NAT, *Network Address Translation*) en el Capítulo 16. Así que las ACLs se ven en la mayoría de los otros exámenes de certificación de Cisco.

Este capítulo trata dos categorías principales de ACLs IP del IOS: estándares y extendidas. Las ACLs estándares utilizan una lógica más simple, y las ACLs extendidas usan una lógica más compleja. La primera sección de este capítulo trata las ACLs IP estándares, seguida por una sección dedicada a las ACLs IP extendidas. Varias secciones relativas a ambos tipos de ACLs cierran el capítulo.

Conceptos de las ACLs IP estándares

Los ingenieros necesitan hacer dos elecciones principales en cualquier ACL que filtre paquetes IP: qué paquetes filtrar, y dónde colocar la ACL dentro de la red. La Figura 6.1 sirve como un ejemplo. En este caso, imagine que Bob no está autorizado a acceder a Server1, pero Larry sí.

La lógica de filtrado se puede configurar en cualquiera de los tres routers y en cualquiera de sus interfaces. Las flechas de línea discontinua en la figura muestran los puntos más apropiados para aplicar la lógica de filtrado en una ACL. Ya que el tráfico de Bob es el único tráfico que necesita ser filtrado, y el objetivo es parar el acceso a Server1, la lista de acceso podría ser aplicada a R1 o a R3. Y ya que el tráfico de Bob hacia Server1 podría no necesitar ir a través de R2, R2 no sería un buen lugar para poner la lógica de la lista de control de acceso. En la discusión, se asume que R1 debe tener la lista de acceso aplicada.

El software IOS de Cisco aplica la lógica de filtrado de una ACL tanto a un paquete entrante por una interfaz como a su salida por la interfaz. Dicho de otra forma, el IOS asocia una ACL con una interfaz, y específicamente al tráfico tanto entrante como saliente de

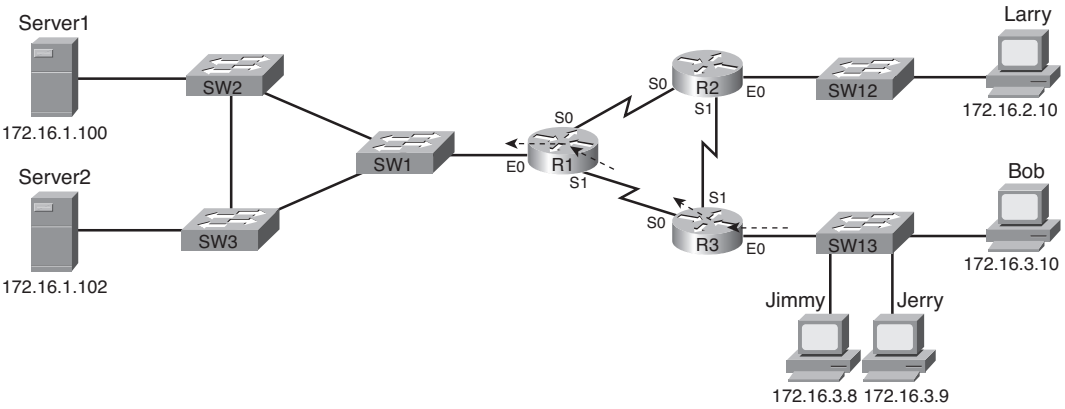


Figura 6.1. Lugares de la red a los que se puede aplicar la lógica de la lista de control de acceso.

la interfaz. Una vez elegido el router en el cual colocar la lista de acceso, se debe elegir la interfaz en la cual aplicar la lógica de acceso, así como si aplicar la lógica para paquetes entrantes o salientes.

Por ejemplo, imagine que desea filtrar los paquetes que Bob envía a Server1. La Figura 6.2. muestra las opciones para filtrar el paquete.

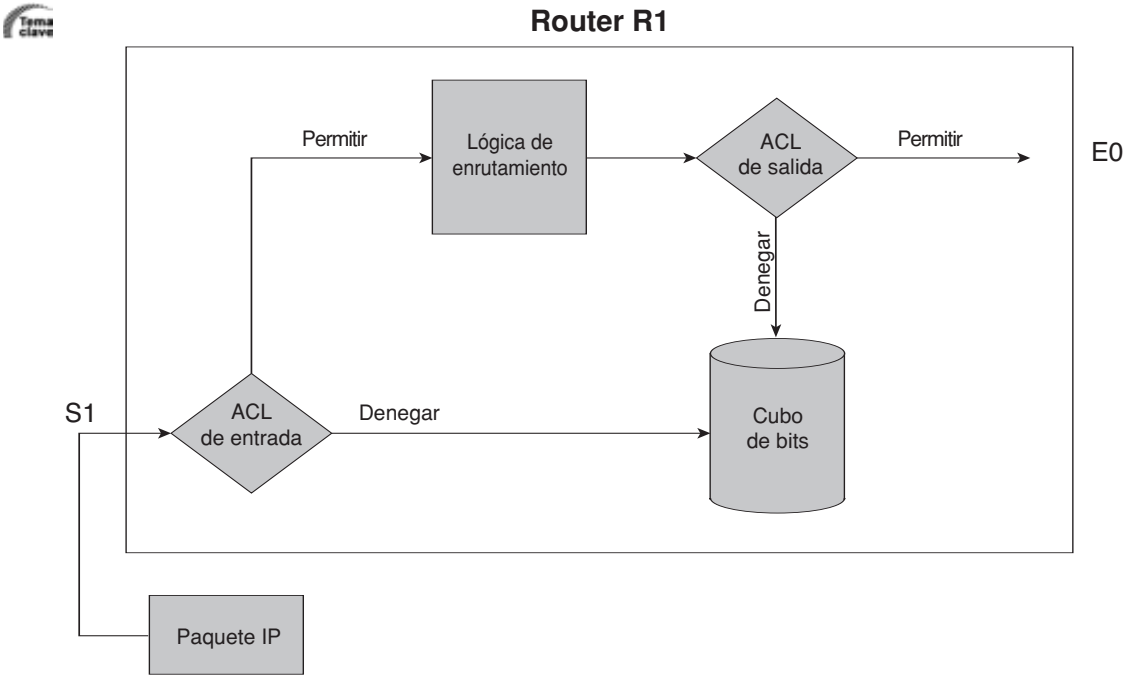


Figura 6.2. Procesamiento Interno en R1 en relación a dónde R1 puede filtrar paquetes.

La lógica de filtrado puede ser aplicada a los paquetes entrantes por S1 o a los paquetes que salen por E0 en R1 para coincidir con los paquetes enviados por Bob a Server1. En general, se puede filtrar paquetes creando y habilitando listas de acceso para los paquetes entrantes y los salientes en cada interfaz. Aquí están algunas de las características clave de las listas de acceso de Cisco:

- Los paquetes pueden ser filtrados cuando entran por una interfaz, antes de la decisión de enrutamiento.
- Los paquetes pueden ser filtrados antes de que salgan por una interfaz, después de la decisión de enrutamiento.
- **Denegar** *(Deny)* es un término utilizado en el software IOS de Cisco para indicar que el paquete será filtrado.
- **Permitir** *(Permit)* es el término usado en el software IOS de Cisco para indicar que el paquete no será filtrado.
- La lógica de filtrado se configura en la lista de acceso.
- Al final de toda la lista de acceso hay una sentencia implícita "denegar todo el tráfico". Por tanto, si un paquete no coincide con ninguna sentencia de la lista de control de acceso, es bloqueado.

Por ejemplo, se puede crear una lista de acceso en R1 y habilitarla en la interfaz S1 de R1. La lista de acceso podría mirar los paquetes que vengan de Bob. Por tanto, la lista de acceso podría necesitar estar habilitada para paquetes entrantes, porque en esta red, los paquetes de Bob entran por S1, y los paquetes para Bob salen por S1.

Las listas de acceso tienen dos pasos principales en su lógica: coincidencia y acción. La lógica de coincidencia examina cada paquete y determina si coincide con la sentencia access-list. Por ejemplo, la dirección IP de Bob podría ser usada para hacer coincidir paquetes enviados por Bob. Las ACLs IP le dicen al router qué acción tomar cuando una sentencia coincide: denegar o permitir. Denegar significa descartar el paquete, y permitir implica que los paquetes continúan su camino.

Así, la lista de acceso para impedir el tráfico de Bob al servidor podría ser algo como esto:

> Mirar los paquetes con dirección IP de origen de Bob y dirección IP de destino de Server1. Cuando se vean, descartarlos. Cualquier otro paquete no descartarlo.

No sorprende que las ACLs IP puedan ser mucho más difíciles que aquellas de la vida real. Incluso una lista de criterios de coincidencia puede crear complicadas listas de acceso en una variedad de interfaces en una variedad de routers. ¡Yo he oído incluso de un par de grandes redes con personal contratado a jornada completa que no hace otra cosa que planear e implementar listas de acceso!

Cisco llama a sus características de filtrado de paquetes "listas de control de acceso", en parte porque la lógica se crea con múltiples comandos de configuración que se consideran en la misma lista. Cuando la lista de acceso tiene múltiples entradas, el IOS busca en la lista secuencialmente la primera sentencia coincidente. La sentencia que coincide determina la acción a tomar. Los dos rombos de la Figura 6.2 representan la aplicación de la lógica de la lista de acceso.

La lógica que el IOS utiliza con una ACL de entrada múltiple puede resumirse como sigue:

1. Comparar los parámetros de coincidencia de la sentencia access-list con el paquete.
2. Si hay coincidencia, realizar la acción definida en esta sentencia access-list (permitir o denegar).
3. Si no hay coincidencia en el Paso 2, repetir los Pasos 1 y 2 con cada sentencia sucesiva de la ACL hasta que exista una coincidencia.
4. Si no hay coincidencia con una entrada de la lista de acceso, realizar la acción de denegar.

Máscaras *wildcard*

Las ACLs IP del IOS buscan la coincidencia de paquetes mirando las cabeceras de IP, TCP y UDP del paquete. Las listas de acceso extendidas pueden verificar direcciones IP de origen y de destino, así como números de puerto de origen y destino, junto con algunos otros campos. Sin embargo, las listas de acceso IP estándares sólo pueden examinar la dirección IP de origen.

Con independencia del uso de ACLs IP estándares o extendidas, se puede decir al router que busque la coincidencia basándose en la dirección IP completa o sólo en una parte de la dirección IP. Por ejemplo, si se desea que Bob detenga el envío de paquetes a Server1, se debe mirar en la dirección IP de Bob y de Server1 entera en la lista de acceso. Pero, ¿cuál sería el criterio para que ningún host de la subred de Bob pueda acceder a Server1? Ya que todos los hosts en la subred de Bob tienen el mismo número en sus tres primeros octetos, la lista de control de acceso podría verificar con un único comando access-list los tres primeros octetos de la dirección para buscar la coincidencia de todos los paquetes.

La **máscara *wildcard*** de Cisco define la porción de la dirección IP que será examinada. Cuando se definen las sentencias ACL, como se verá en la siguiente sección de este capítulo, se puede definir una máscara *wildcard* junto con la dirección IP. La máscara *wildcard* le dice al router qué parte de la dirección IP de la sentencia de configuración debe ser comparada con la cabecera del paquete.

Por ejemplo, suponer que una máscara implica que el paquete entero debe ser verificado y otra implica que sólo los tres primeros octetos de la dirección necesitan ser examinados. (Para hacer esto se puede elegir hacer coincidir todos los hosts IP en la misma subred cuando se utiliza una máscara de 255.255.255.0.) Para comprobar esta coincidencia, las listas de acceso de Cisco utilizan máscaras *wildcard*.

Las máscaras *wildcard* son similares a las máscaras de subred, pero no iguales. Las máscaras *wildcard* representan un número de 32 bits, al igual que las máscaras de subred. Sin embargo, la máscara *wildcard* de 0 bits le dice al router que los bits correspondientes en la dirección deben ser comparados cuando se realiza la lógica de coincidencia. Los 1s binarios de la máscara *wildcard* le dice al router que estos bits no necesitan ser comparados.

Para dar sentido a la idea de una máscara *wildcard*, la Tabla 6.2 lista algunas de las máscaras *wildcard* más comunes, junto con su significado.

Tabla 6.2. Ejemplos de máscaras *wildcard* en la lista de acceso.

Máscara *wildcard*	**Versión binaria de la máscara**	**Descripción**
0.0.0.0	00000000.00000000.00000000.00000000	La dirección IP completa debe coincidir.
0.0.0.255	00000000.00000000.00000000.11111111	Los primeros 24 bits deben coincidir.
0.0.255.255	00000000.00000000.11111111.11111111	Los primeros 16 bits deben coincidir.
0.255.255.255	00000000.11111111.11111111.11111111	Los primeros 8 bits deben coincidir.
255.255.255.255	11111111.11111111.11111111.11111111	Automáticamente considerada para coincidir con todas las direcciones.
0.0.15.255	00000000.00000000.0001111.11111111	Los primeros 20 bits deben coincidir.
0.0.3.255	00000000.00000000.0000011.11111111	Los primeros 22 bits deben coincidir.

Los primeros ejemplos muestran un uso típico de la máscara *wildcard*. Como se puede ver, no es una máscara de subred. Un *wildcard* de 0.0.0.0 significa que se debe examinar la dirección IP entera, y ser igual, para ser considerada una coincidencia. 0.0.0.255 significa que el último octeto automáticamente coincide, pero los 3 primeros deben ser examinados, y así sucesivamente. De forma más general, la máscara *wildcard* significa lo siguiente:

> Las posiciones de bit con 0 binario significa que la lista de acceso compara las posiciones de bit correspondientes de la dirección IP y se asegura que son iguales a las mismas posiciones de bit en la dirección configurada en la sentencia access-list. Las posiciones de bit con 1 binario son bits por los que no hay que preocuparse. Estas posiciones de bit son inmediatamente consideradas una coincidencia.

Las dos últimas filas de la Tabla 6.2 muestran dos razonables, pero no obvias, máscaras *wildcard*. 0.0.15.255 en binario es 20 ceros binarios seguidos de 12 unos binarios. Esto significa que los primeros 20 bits deben coincidir. De forma similar, 0.0.3.255 significa que se deben examinar los primeros 22 bits para ver si coinciden. ¿Por qué son útiles? Si la máscara de subred es 255.255.240.0, y se desea hacer coincidir a todos los hosts en la misma subred, el *wildcard* 0.0.15.255 significa que todos los bits de red y subred deben coincidir, y todos los bits de host son considerados automáticamente como coincidentes. Igualmente, si se desea filtrar todos los hosts de una subred que utiliza la máscara de subred 255.255.252.0, la máscara *wildcard* 0.0.3.255 hace coincidir los bits de red y subred. En general, si desea una máscara *wildcard* que le ayude a hacer coincidir todos

los host de una subred, invierta la máscara de subred, y tendrá la máscara *wildcard* correcta.

Una alternativa rápida para interpretar máscaras *wildcard*

Tanto las ACLs IP estándares (solamente dirección IP de origen) como las ACLs extendidas (direcciones de origen y de destino) se pueden configurar para examinar toda o parte de una dirección IP basándose en máscaras *wildcard*. Sin embargo, en concreto para los exámenes, trabajar con las máscaras en binario puede ser lento y laborioso a menos que se dominen las conversiones de binario a decimal y de decimal a binario. Esta sección sugiere un método fácil de trabajo con máscaras *wildcard* ACL que funciona bien si ya domina la matemática de las subredes.

En muchos casos, una ACL necesita coincidir con todos los hosts de una subred particular. Para hacer coincidir una subred con una ACL, se puede usar el siguiente atajo:

- Utilice el número de subred como el valor de dirección en el comando access-list.
- Utilice una máscara *wildcard* igual al resultado de restar a 255.255.255.255 la máscara de subred.

Por ejemplo, para la subred 172.16.8.0 255.255.252.0, utilice el número de subred (172.16.8.0) como el parámetro **dirección**, y después realice la siguiente operación para encontrar la máscara *wildcard*:

```
  255.255.255.255
– 255.255.252.0
-----------------
    0.   0.   3.255
```

Algunas preguntas del examen pueden no preguntar la sentencia ACL que se necesita para configurarla; en cambio preguntan que se interprete la salida de algunos comandos access-list existentes. Normalmente, estas preguntas muestran sentencias ACL preconfiguradas, o se necesita mostrar el contenido de una ACL de un simulador de router, y se necesita decidir que sentencia coincide con un paquete en particular. Para hacer esto, es necesario determinar el rango de direcciones IP que coinciden con una combinación dirección/máscara *wildcard* en concreto con cada sentencia ACL.

Si se domina la matemática de subred usando algún atajo decimal, evitando la matemática binaria, se puede utilizar otro atajo para analizar cada par dirección/*wildcard* en cada comando ACL. Para hacer esto:

Paso 1 Utilice la dirección en el comando access-list como si fuera un número de subred.

Paso 2 Utilice como máscara de subred el número resultante de restar a 255.255.255.255 la máscara *wildcard*.

Paso 3 Trate los valores de los dos primeros pasos como un número de subred y máscara de subred, y encuentre la dirección de difusión de la subred. La ACL hace

corresponder el rango de direcciones entre el número de subred y la dirección de difusión, ambos incluidos.

El rango de direcciones identificado por este proceso es el mismo rango de direcciones identificadas por la ACL. Por tanto, si se desea encontrar un rango de direcciones de subredes rápida y fácilmente, este proceso puede ayudarle a responder más rápidamente en los exámenes. Por ejemplo, con el comando access-list 1 permit 172.16.200.0 0.0.7.255, podría pensar primero en 172.16.200.0 como un número de subred. Después podría calcular la máscara de subred asumida, 255.255.248.0, como sigue:

```
  255.255.255.255
– 0.   0.   7.255
---------------
  255.255.248.0
```

Desde aquí, usando el proceso que desee, utilice la matemática de subredes para determinar que la dirección de difusión de esta subred podría ser 172.16.207.255. Por tanto, el rango de direcciones coincidente con esta sentencia ACL podría ser de 172.16.200.0 hasta 172.16.207.255.

Nota

El Escenario 3 apéndice F, disponible sólo en el DVD, proporciona una oportunidad de practicar la elección de una máscara *wildcard* para coincidir con los hosts de una subred particular.

Configuración de las listas de acceso IP estándares

La configuración ACL tiende a ser más simple que la tarea de interpretar el significado y las acciones tomadas por una ACL. Para este fin, esta sección presenta un plan de ataque para configurar ACLs. Después muestra un par de ejemplos que revisan la configuración y los conceptos implementados por estas ACLs.

La sintaxis genérica del comando de configuración ACL estándar es:

access-list *número-lista-acceso* {deny | permit} *origen* [*wildcard-origen*]

Una lista de acceso estándar utiliza una serie de comandos access-list que tienen el mismo nombre. Los comandos access-list con el mismo número se consideran en la misma lista, con los comandos listados en el mismo orden en el cual se añaden a la configuración. Cada comando access-list puede coincidir con un rango de direcciones IP de origen. Si hay una coincidencia, la ACL o bien permite la circulación del paquete (acción permit) o lo descarta (acción deny). Cada ACL estándar puede coincidir con toda o con sólo una parte de la dirección IP de origen del paquete. Observe que para las ACLs IP estándares, el rango de números para las ACLs es de 1 a 99 y de 1300 a 1999.

La lista siguiente sugiere un proceso de configuración. No necesita memorizar este proceso para el examen; simplemente lo mostramos aquí como una ayuda de estudio.

Paso 1 Planifique la localización (router e interfaz) y la dirección (entrante o saliente) en esa interfaz:

- **a.** Las ACLs estándares deben ponerse cerca del destino de los paquetes para que no deseche involuntariamente paquetes que no deben desecharse.
- **b.** Ya que las ACLs estándares sólo pueden coincidir con una dirección IP de origen del paquete, identificar las direcciones IP de origen de los paquetes según van en la dirección que la ACL está examinando.

Paso 2 Configurar uno o más comandos globales de configuración access-list para crear la ACL, teniendo lo siguiente en mente:

- **a.** La búsqueda en la lista es secuencial, utilizando la lógica de primera coincidencia. Dicho de otra forma, cuando los paquetes coinciden con una sentencia access-list, la búsqueda ha terminado, aunque el paquete pudiera coincidir con sentencias posteriores.
- **b.** La acción predeterminada, si el paquete no coincide con ninguno de los comandos access-list, es deny (descartar) el paquete.

Paso 3 Habilitar la ACL en la interfaz del router elegido, en la dirección correcta, utilizando el subcomando de interfaz ip access-group *número* {in | out}.

A continuación se muestran dos ejemplos de ACLs estándar.

Ejemplo 1 de ACL IP estándar

El Ejemplo 6.1. intenta parar el tráfico desde Bob a Server1. Como se muestra en la Figura 6.1, Bob no está autorizado a acceder a Server1. En el Ejemplo 6.1, la configuración habilita una ACL para todos los paquetes salientes por la Ethernet0 de R1. La ACL coincide con la dirección origen del paquete: dirección IP de Bob. Observe que los comandos access-list están en la parte inferior del ejemplo porque el comando show running-config también los lista cerca de la parte inferior, después de los comandos de configuración de interfaz.

Ejemplo 6.1. Lista de acceso estándar en R1 para impedir que Bob alcance Server1.

```
interface Ethernet0
 ip address 172.16.1.1 255.255.255.0
 ip access-group 1 out
!
access-list 1 remark detener todo el tráfico cuyo origen IP es Bob
access-list 1 deny 172.16.3.10 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255
```

Primero, nos centraremos en la sintaxis básica de los comandos. Las listas de acceso IP estándares utilizan un número en el rango de 1 a 99 ó de 1300 a 1999. Este ejemplo utiliza la ACL número 1 en vez de otros números disponibles por ninguna razón en particular. (No hay

absolutamente ninguna diferencia en utilizar un número u otro, con tal de que esté en el rango correcto. Dicho de otra forma, la lista 1 no es ni mejor ni peor que la lista 99.) Los comandos access-list, con los cuales se define la coincidencia y la lógica de la acción, son comandos de configuración global. Para habilitar la ACL en una interfaz y definir la dirección de los paquetes para los cuales se aplica la ACL, se utiliza el comando ip access-group. En este caso, se habilita la lógica para la ACL 1 en Ethernet0 para los paquetes salientes por la interfaz.

La ACL 1 evita que los paquetes enviados por Bob salgan por la interfaz Ethernet de R1, basándose en la lógica de coincidencia del comando access-list 1 deny 172.16.3.10 0.0.0.0. La máscara *wildcard* 0.0.0.0 significa "coincidencia de todos los 32 bits"; por tanto, sólo los paquetes cuya dirección IP coincida exactamente con 172.16.3.10 coinciden con esta sentencia y son descartados. El comando access-list 1 permit 0.0.0.0 255.255.255.255, la última sentencia de la lista, coincide con todos los paquetes, porque la máscara *wildcard* 255.255.255.255 significa "no preocuparse" de los 32 bits. Dicho de otra forma, la sentencia coincide con todas las direcciones IP de origen. Estos paquetes están permitidos.

Finalmente, observe que el ingeniero también añade un comando access-list 1 remark a la ACL. Este comando permite añadir un comentario que permita hacer el seguimiento del propósito de la ACL. El comentario sólo se muestra en la configuración; no se lista en la salida del comando show.

Aunque es un ejemplo aparentemente sencillo, en este caso la lista de acceso 1 también impide que se entreguen los paquetes de Bob enviados a Server2. Con la topología mostrada en la Figura 6.1, una ACL estándar de salida en la interfaz E0 de R1 no puede negar a Bob el acceso de algún modo a Server1 mientras permite el acceso a Server2. Para hacer esto, se necesita una ACL extendida que pueda comprobar las direcciones IP de origen y de destino.

De forma interesante, si los comandos del Ejemplo 6.1 se introducen desde el modo de configuración, el IOS cambia la sintaxis de configuración de un par de comandos. La salida del comando show running-config del Ejemplo 6.2 muestra lo que el IOS coloca exactamente en el fichero de configuración.

Ejemplo 6.2. Lista de acceso estándar revisada para impedir que Bob alcance Server1.

```
interface Ethernet0
 ip address 172.16.1.1 255.255.255.0
 ip access-group 1 out

access-list 1 remark detener todo el tráfico cuyo origen IP es Bob
access-list 1 deny host 172.16.3.10
access-list 1 permit any
```

Los comandos del Ejemplo 6.1 cambian basándose en tres factores. El IOS de Cisco permite tanto un estilo antiguo como un estilo nuevo de configuración para algunos parámetros. El Ejemplo 6.1 muestra el estilo antiguo, y el router cambia al estilo nuevo equivalente de configuración en el Ejemplo 6.2. Primero, el uso de la máscara *wildcard* 0.0.0.0 significa de hecho que el router debe coincidir con esa dirección IP de host específica. El nuevo estilo de configuración utiliza la palabra clave host **delante** de la dirección IP especificada.

El otro cambio en el nuevo estilo de configuración tiene que ver con el uso de la máscara *wildcard* 255.255.255.255 con el significado "coincidencia de cualquier cosa". El nuevo estilo de configuración utiliza la palabra clave any para reemplazar la dirección IP y la máscara *wildcard* 255.255.255.255. any simplemente significa coincidencia con cualquier dirección IP.

Ejemplo 2 de ACL IP estándar

El segundo ejemplo de ACL IP estándar expone más problemas. La Figura 6.3 y los Ejemplos 6.3 y 6.4 muestran un uso básico de las listas de acceso IP estándares, con dos precauciones típicas en el primer esfuerzo hacia una solución completa. Los criterios de las listas de acceso son los siguientes:

- Sam no está autorizado a acceder ni a Bugs ni a Daffy.
- Los hosts en la Ethernet Seville no tienen permiso para acceder a los hosts de la Ethernet de Yosemite.
- Se permite cualquier otra combinación.

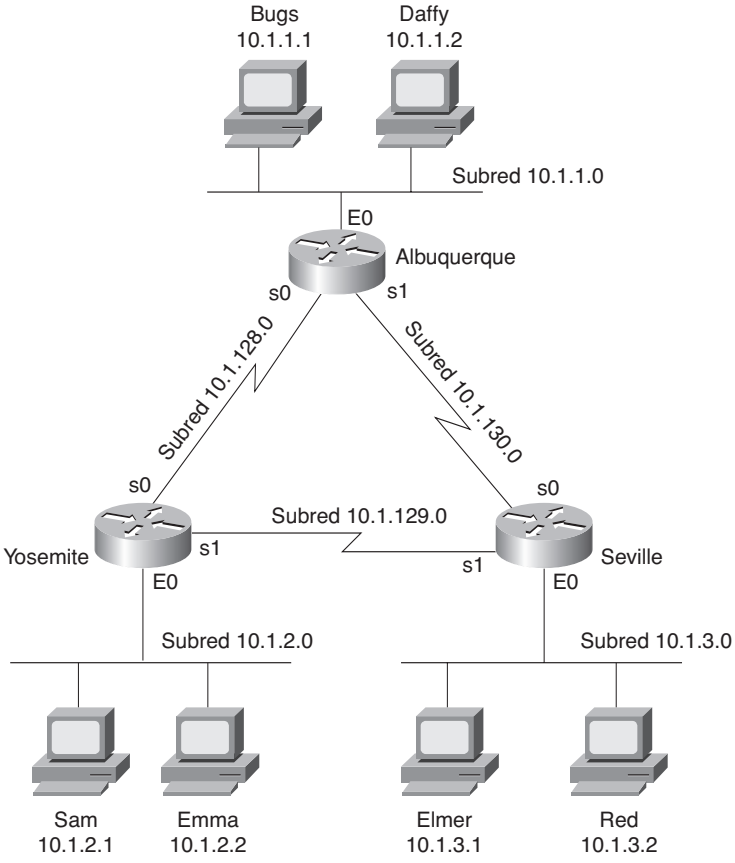


Figura 6.3. Diagrama de red para el ejemplo de lista de acceso estándar.

Ejemplo 6.3. Configuración de Yosemite para el ejemplo de la lista de acceso estándar.

```
interface serial 0
 ip access-group 3 out
!
access-list 3 deny host 10.1.2.1
access-list 3 permit any
```

Ejemplo 6.4. Configuración de Seville para el ejemplo de la lista de acceso estándar.

```
interface serial 1
 ip access-group 4 out
!
access-list 4 deny 10.1.3.0 0.0.0.255
access-list 4 permit any
```

A primera vista, estas dos listas de acceso parecen realizar las funciones deseadas. La ACL 3 permite que los paquetes salientes por la interfaz S0 de Yosemite, tengan en cuenta el criterio 1, porque la ACL 3 coincide exactamente con la dirección IP de Sam. La ACL 4 en Seville permite que los paquetes salientes por su interfaz S1 tengan en cuenta el criterio 2, porque la ACL 4 coincide con todos los paquetes procedentes de la subred 10.1.3.0/24. Ambos routers cumplen con el criterio 3: se utiliza un comodín permit any al final de cada lista de acceso para reescribir lo predeterminado, que es descartar todos los demás paquetes. Por tanto, parece que se cumplen todos los criterios.

Sin embargo, cuando un enlace de la WAN falla, pueden aparecer algunos agujeros en las ACLs. Por ejemplo, si el enlace de Albuquerque a Yosemite falla, Yosemite aprende una ruta a 10.1.1.0/24 a través de Seville. Los paquetes de Sam, enviados por Yosemite y destinados a los hosts de Albuquerque, dejan la interfaz serial 1 de Yosemite sin ser filtrados. Así, el criterio 1 no se vuelve a cumplir. De forma similar, si el enlace de Seville a Yosemite falla, Seville enruta los paquetes a través de Albuquerque, ignorando la lista de acceso habilitada en Seville, de modo que el criterio 2 ya no se cumple.

El Ejemplo 6.5. muestra una solución alternativa, con toda la configuración realizada en Yosemite; una que funciona incluso cuando algún enlace falle.

La configuración mostrada en el Ejemplo 6.5. soluciona el problema de los Ejemplos 6.3. y 6.4. La ACL 3 comprueba la dirección IP de origen de Sam, y está habilitada en ambos enlaces serie para el tráfico de salida. Así, para el tráfico que es reencaminado porque un enlace WAN falla, los paquetes de Sam todavía se filtran. Para lograr el criterio 2, Yosemite filtra los paquetes que salen por su interfaz Ethernet. Por tanto, independientemente de por cuál de los dos enlaces WAN lleguen los paquetes, los paquetes de la subred de Seville no son reenviados a la Ethernet de Yosemite.

Ejemplo 6.5. Ejemplo de configuración de Yosemite para la lista de acceso estándar: solución alternativa para los Ejemplos 6.3 y 6.4

```
interface serial 0
 ip access-group 3 out
!
interface serial 1
 ip access-group 3 out
!
interface ethernet 0
 ip access-group 4 out
!
access-list 3 remark cumplir criterio 1
access-list 3 deny host 10.1.2.1
access-list 3 permit any
!
access-list 4 remark cumplir criterio 2
access-list 4 deny 10.1.3.0 0.0.0.255
access-list 4 permit any
```

Listas de control de acceso IP extendidas

Las listas de acceso IP extendidas tienen similitudes y diferencias comparándolas con las ACLs IP estándares. Al igual que las listas estándares, se habilitan listas de acceso extendidas en las interfaces para los paquetes que entran o salen por una interfaz. El IOS busca secuencialmente en la lista. La primera sentencia que coincide finaliza la búsqueda en la lista y define la acción a tomar. Todas estas características son ciertas también para las listas de acceso estándares.

Una diferencia clave entre las dos es la variedad de campos del paquete que se pueden comparar con las listas de acceso extendidas. Una única sentencia de ACL extendida puede examinar varias partes del encabezado del paquete, necesitando que todos los parámetros coincidan correctamente para que esta sentencia de ACL sea coincidente. Esta lógica de coincidencia es la que hace a las listas de acceso extendidas más útiles y más complejas que las ACLs IP estándares.

Esta sección comienza tratando los conceptos de las ACL IP extendidas que las diferencia de las ACLs estándares; lo denominado lógica de coincidencia. Después de esto, se tratan los detalles de configuración.

Conceptos de las ACL IP extendidas

Las listas de acceso extendidas crean una lógica de coincidencia poderosa examinando muchas partes de un paquete. La Figura 6.4. muestra varios campos de la cabecera del paquete que pueden coincidir.

El conjunto superior de campos de cabecera muestra el tipo de protocolo IP, que identifica que la cabecera siguiente es la cabecera IP. Se puede especificar todos los campos de

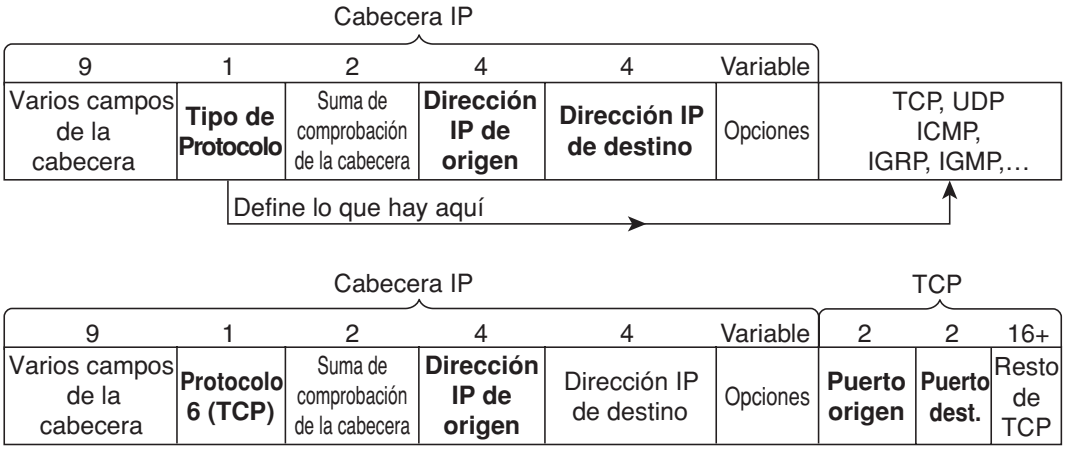


Figura 6.4. Opciones de Coincidencia de las Listas de acceso Extendidas.

los paquetes IP, o aquellos de la cabecera TCP, UDP, ICMP, etcétera, verificando el campo Protocolo. Se puede también verificar las direcciones IP de origen y de destino, como se muestra. La parte inferior de la figura muestra un ejemplo de cabecera TCP a continuación de la cabecera IP, señalando la localización de los números de puerto de origen y de destino TCP. Estos números de puerto identifican la aplicación. Por ejemplo, la web utiliza el puerto 80 de forma predeterminada. Si se especifica un protocolo TCP o UDP, también se puede verificar el número de puerto.

La Tabla 6.3 resume los campos más comunes que se pueden utilizar para buscar una coincidencia en una ACL IP extendida, en comparación con las ACLs IP estándares.

Tabla 6.3. Listas de acceso IP estándares y extendidas: coincidencias.

Tipo de lista de acceso	Qué puede coincidir
ACLs estándares y extendidas	Dirección IP de origen
	Porciones de la dirección IP de origen utilizando máscaras *wildcard*
Sólo ACLs extendidas	Dirección IP de destino
	Porciones de la dirección IP de destino usando máscaras *wildcard*
	Tipo de protocolo (TCP, UDP, ICMP, IGRP, IGMP, y otros)
	Puerto de origen
	Puerto de destino
	Todos los flujos TCP excepto el primero
	TOS IP
	Precedencia de IP

Conocer qué buscar es sólo la mitad de la batalla. El IOS comprueba toda la información coincidente configurada en un único comando access-list. Todo debe coincidir con este único comando para ser considerado una coincidencia y para que se realice la acción definida. Las opciones comienzan con el tipo de protocolo (IP, TCP, UDP, ICMP, y otros), seguido de la dirección IP de origen, el puerto de origen, la dirección IP de destino, y el número de puerto de destino. La Tabla 6.4 lista varios ejemplos de comandos access-list, con varias opciones configuradas y una explicación. Sólo las opciones que coinciden aparecen sombreadas.

Tabla 6.4. Comandos **access-list** extendidos y explicaciones de la lógica.

Sentencia access-list	Con qué coincide
access-list 101 deny ip any host 10.1.1.1	Cualquier paquete IP, cualquier dirección IP de origen, con una dirección IP de destino 10.1.1.1.
access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23	Paquetes con una cabecera TCP, cualquier dirección IP de origen, con un puerto de origen mayor que (gt) 1023, una dirección IP de destino exactamente igual a 10.1.1.1, y un puerto de destino igual a (eq) 23.
access-list 101 deny tcp any host 10.1.1.1 eq 23	Lo mismo que el ejemplo anterior, pero coincide con cual quier puerto de origen, porque en este caso se omite el parámetro.
access-list 101 deny tcp any host 10.1.1.1 eq telnet	Lo mismo que el ejemplo anterior. La palabra clave telnet se utiliza en lugar del puerto 23.
access-list 101 deny udp 1.0.0.0 0.255.255.255 lt 1023 any	Un paquete con origen en la red 1.0.0.0, usando UDP con un puerto de origen menor que (lt) 1023, con cualquier dirección IP de destino.

Coincidencias de los números de puerto TCP y UDP

Las ACLs IP extendidas permiten la coincidencia del campo de protocolo de la cabecera IP, así como la coincidencia de los números de puerto TCP o UDP de origen y de destino. Sin embargo, mucha gente tiene dificultades cuando configura por primera vez ACLs que coincidan con números de puerto, concretamente cuando coinciden con el número de puerto de origen.

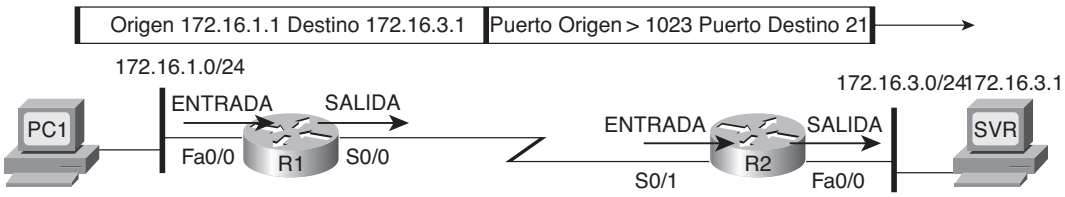
Cuando se plantee cualquier pregunta de examen en la que se vean implicados puertos TCP o UDP, tenga en mente estos puntos clave:

- El comando access-list debe utilizar la palabra clave tcp para habilitar la coincidencia de puertos TCP y la palabra clave udp para habilitar la coincidencia de puertos UDP. La palabra clave ip no está permitida para coincidir con los números de puerto.

- Los parámetros de puerto de origen y de destino en el comando access-list son posicionales. Dicho de otra forma, su lugar en el comando determina si el parámetro examina el puerto de origen o el de destino.
- Recuerde que las ACLs pueden coincidir con paquetes enviados a un servidor comparando el puerto de destino con el número de puerto bien conocido. Sin embargo, las ACLs necesitan coincidir con el puerto de origen de los paquetes enviados por el servidor.
- Es útil memorizar las aplicaciones TCP y UDP más comunes, y sus puertos bien conocidos, como las especificadas en la Tabla 6.5 que se encuentra más adelante en este capítulo.

Por ejemplo, considérese la sencilla red que se muestra en la Figura 6.5: el servidor FTP situado a la derecha, y el cliente a la izquierda. La figura muestra la sintaxis de una ACL que coincide con:

- Paquetes que incluyen una cabecera TCP.
- Paquetes enviados desde la subred cliente.
- Paquetes enviados a la subred servidora.
- Paquetes con el puerto de destino 21 de TCP.

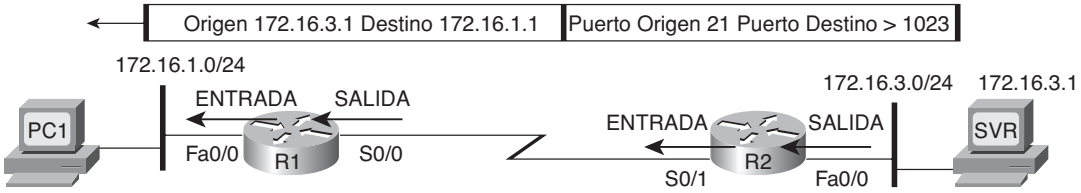


access-list 101 permit tcp 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21

Figura 6.5. Filtrando paquetes basándose en el puerto de destino.

Para apreciar completamente la coincidencia con el puerto de destino con el parámetro eq 21, considérense paquetes moviéndose de izquierda a derecha, desde PC1 hacia el servidor. Si el servidor está utilizando el puerto bien conocido 21 (puerto de control de FTP), el paquete enviado por PC1, en la cabecera TCP, tiene un valor 21 en el puerto de destino. La sintaxis de la ACL incluye el parámetro eq 21 **después** de la dirección IP de destino; con esta posición en el comando implica que este parámetro coincide con el puerto de destino. Como resultado, la sentencia ACL mostrada en la figura podría coincidir con este paquete, y el puerto de destino 21, si se utiliza en cualquiera de los cuatro lugares señalados por las cuatro fechas de la figura.

Recíprocamente, la Figura 6.6 muestra el flujo inverso, con un paquete enviado de vuelta por el servidor hacia PC1. En este caso, la cabecera TCP del paquete tiene un puerto origen igual a 21; por tanto, la ACL debe comprobar si el valor del puerto de origen es 21, y la ACL debe colocarse en diferentes interfaces.



access-list 101 permit tcp 172.16.3.0 0.0.0.255 eq 21 172.16.1.0 0.0.0.255

Figura 6.6. Filtrado de paquetes basándose en el puerto de origen.

Para las preguntas del examen en las que se necesiten ACLs y coincidencia de números de puerto, primero considere si la pregunta necesita que la ACL se coloque en un cierto lugar y dirección. Si es así, debe determinar si esta ACL podría procesar paquetes tanto enviados al servidor como enviados por éste. En este punto, puede decidir si necesita comprobar el puerto de origen o de destino del paquete.

Como referencia, la Tabla 6.5 lista muchos de los números de puerto más comunes y sus protocolos de transporte y aplicaciones. Observe que la sintaxis de los comandos

Tabla 6.5 Aplicaciones más comunes y sus números de puerto bien conocidos.

Número(s) de puerto	Protocolo	Aplicación	Palabra clave del nombre de la aplicación en la sintaxis del comando access-list
20	TCP	Datos FTP	ftp-data
21	TCP	Control FTP	ftp
22	TCP	SSH	—
23	TCP	Telnet	telnet
25	TCP	SMTP	smtp
53	UDP, TCP	DNS	domain
67, 68	UDP	DHCP	nameserver
69	UDP	TFTP	tftp
80	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	snmp
443	TCP	SSL	—
16.384-32.767	UDP	Voz basada en RTP (VoIP) y vídeo	—

access-list acepta tanto los números de puerto como una versión taquigráfica del nombre de la aplicación.

Configuración de las ACLs IP extendidas

Debido a que las ACLs pueden coincidir con varios campos diferentes de varias cabeceras de un paquete IP, la sintaxis del comando no se puede resumir fácilmente en un único comando genérico. Como referencia, la Tabla 6.6 muestra la sintaxis de los dos comandos genéricos más comunes.

Tabla 6.6. Comandos de configuración de las listas de acceso IP extendidas.

Comando	Modo de configuración y descripción
acces-list *número-lista-acceso* {deny | permit} *protocolo origen wildcard-origen destino wildcard-destino* [log | log-input]	Comando global para listas de acceso extendidas numeradas. Utiliza un número entre 100 y 199 ó 2000 y 2699, incluidos.
acces-list *número-lista-acceso* {deny | permit} {tcp | udp} *origen wildcard-origen* [*operador* [*puerto*]] *destino wildcard-destino* [*operador* [*puerto*]] [established] [log]	Una versión del comando access-list con parámetros específicos de TCP.

El proceso de configuración para las ACLs extendidas coincide con el proceso utilizado para las ACLs estándares. La ubicación y dirección se deben elegir primero para poder planificar los parámetros de la ACL basándose en la información de los paquetes que fluyen en esa dirección. La ACL se configura con los comandos access-list. Entonces la ACL se puede habilitar con el mismo comando ip access-group usado en las ACLs estándares. Todos estos pasos son los mismos que en las ACLs estándares. Las diferencias en la configuración se resumen a continuación:

- Las ACLs extendidas se deben situar lo más cerca posible del origen de los paquetes a filtrar, ya que las ACLs extendidas se pueden configurar para que no descarten paquetes que no deban ser descartados. Por tanto, filtrar cerca del origen de los paquetes ahorra algo de ancho de banda.
- Todos los campos de un único comando access-list deben coincidir con un paquete para que ese paquete se considere coincidente con esta sentencia access-list.
- El comando access-list extendido utiliza números entre 100-199 y 2000-2699, con ningún número mejor que otro.

La versión extendida del comando access-list permite para la coincidencia de números de puerto el uso de varias operaciones básicas, tales como igual a y menor que. Sin embargo, los comandos utilizan abreviaturas. La Tabla 6.7 muestra las abreviaturas y una explicación más completa.

Tema clave

Tabla 6.7. Operadores utilizados en la comparación de números de puerto.

Operador en el comando access-list	Significado
eq	Igual a
neq	No igual a
lt	Menor que
gt	Mayor que
range	Rango de números de puerto

Ejemplo 1 de listas de acceso IP extendidas

Este ejemplo se centra en entender la sintaxis básica. En este caso, Bob tiene denegado el acceso a todos los servidores FTP de la Ethernet de R1, y Larry no tiene acceso al servidor web de Server1. La Figura 6.7 es un recordatorio de la topología de la red. El Ejemplo 6.6 muestra la configuración de R1.

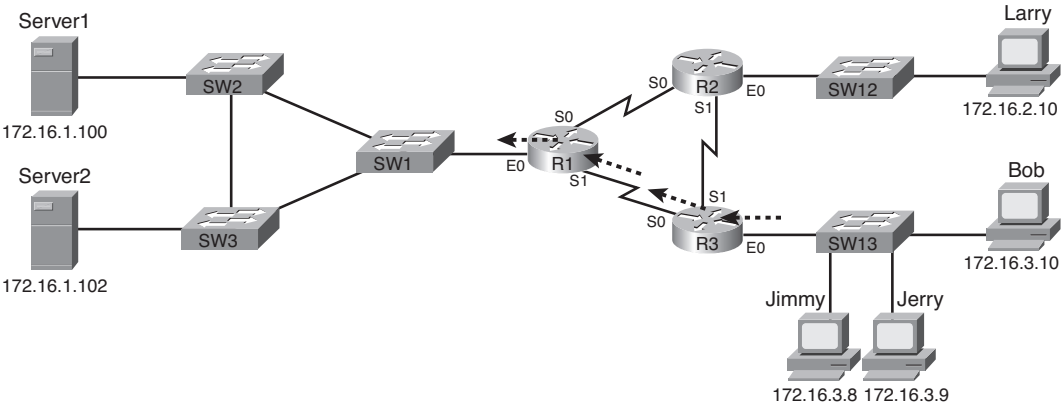


Figura 6.7. Diagrama de red para el Ejemplo 1 de listas de acceso extendidas.

Ejemplo 6.6. Lista de acceso extendida de R1: Ejemplo 1.

```
interface Serial0
 ip address 172.16.12.1 255.255.255.0
 ip access-group 101 in
!
interface Serial1
 ip address 172.16.13.1 255.255.255.0
 ip access-group 101 in
!
```

(continúa)

Ejemplo 6.6. Lista de acceso extendida de R1: Ejemplo 1 *(continuación).*

```
access-list 101 remark detener Bob a servidores FTP, y a Larry a web Server1
access-list 101 deny tcp host 172.16.3.10 172.16.1.0 0.0.0.255 eq ftp
access-list 101 deny tcp host 172.16.2.10 host 172.16.1.100 eq www
access-list 101 permit ip any any
```

En el Ejemplo 6.6, la primera sentencia ACL previene el acceso de Bob a los servidores FTP en la subred 172.16.1.0. La segunda sentencia previene el acceso de Larry a los servicios web de Server1. La sentencia final permite cualquier otro tráfico.

Centrándonos por un momento en la sintaxis, existen varios nuevos elementos a revisar. Primero, el número de la lista de acceso para las listas de acceso extendidas está en el rango de 100 a 199 ó de 2000 a 2699. Seguido de la acción permit o deny, el parámetro *protocolo* define si se desea verificar todos los paquetes IP o sólo aquellos con cabeceras TCP o UDP. Cuando se validan números de puerto TCP o UDP, se debe especificar el protocolo TCP o UDP.

Este ejemplo utiliza el parámetro eq, que significa "igual", para comprobar los números de puerto de destino para controlar FTP (palabra clave ftp) y el tráfico HTTP (palabra clave www). Se puede utilizar el valor numérico o, para las opciones más populares, es válida una versión de texto más obvia. (Si se especificara eq 80, la configuración mostraría eq www.)

En este primer ejemplo de ACL extendida, las listas de acceso podrían haberse situado en R2 y R3 en lugar de en R1. Como podrá leer cerca del final de este capítulo, Cisco realiza unas recomendaciones específicas de dónde situar las ACLs IP. Con las ACLs IP extendidas, Cisco sugiere que se coloquen lo más cerca posible del origen del paquete. Por tanto, el Ejemplo 6.7 consigue el mismo objetivo que el Ejemplo 6.6 de impedir el acceso de Bob a los servidores FTP del sitio principal, y lo hace con una ACL en R3.

Ejemplo 6.7. Lista de acceso extendida de R3 impidiendo a Bob alcanzar los servidores de FTP cerca de R1.

```
interface Ethernet0
 ip address 172.16.3.1 255.255.255.0
 ip access-group 101 in

access-list 101 remark denegar Bob a servidores FTP en la subred 172.16.1.0/24
access-list 101 deny tcp host 172.16.3.10 172.16.1.0 0.0.0.255 eq ftp
access-list 101 permit ip any any
```

La ACL 101 se parece mucho a la ACL 101 del Ejemplo 6.6, pero esta vez, la ACL no molesta para verificar el criterio de coincidencia del tráfico de Larry, puesto que el tráfico de Larry nunca entrará por la interfaz Ethernet 0 de R3. Debido a que la ACL está situada en R3, cerca de Bob, busca paquetes enviados por Bob que entren por su interfaz Ethernet0. Debido a la ACL, el tráfico FTP de Bob a 172.16.1.0/24 es denegado, con todo el otro tráfico entrando en la red por la interfaz E0 de R3. El Ejemplo 6.7 no muestra ninguna lógica para parar el tráfico de Larry.

Ejemplo 2 de listas de acceso IP extendidas

El Ejemplo 6.8, basado en la red mostrada en la Figura 6.8, muestra otro ejemplo de cómo utilizar las listas de acceso IP extendidas. Este ejemplo utiliza el mismo criterio y topología de red que el segundo ejemplo de ACL IP estándar, como se repite aquí:

- Sam no puede acceder ni a Bugs ni a Daffy.
- Los hosts en la Ethernet Seville no pueden acceder a los hosts de la Ethernet Yosemite.
- Cualquier otra combinación está permitida.

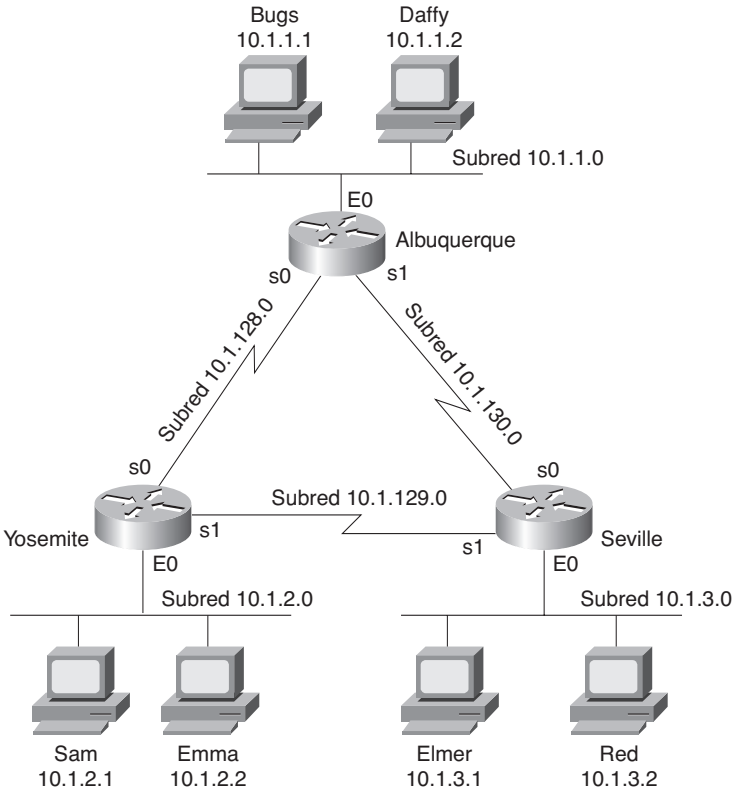


Figura 6.8. Diagrama de red para la lista de acceso extendida del Ejemplo 2.

Ejemplo 6.8. Configuración de Yosemite para la lista de acceso extendida del Ejemplo 2.

```
interface ethernet 0
 ip access-group 110 in
!
access-list 110 deny ip host 10.1.2.1 10.1.1.0 0.0.0.255
access-list 110 deny ip 10.1.2.0 0.0.0.255 10.1.3.0 0.0.0.255
access-list 110 permit ip any any
```

Esta configuración soluciona los problemas con unas pocas sentencias además de seguir las directrices de Cisco de colocar las ACLs extendidas tan cerca como sea posible del origen del tráfico. La ACL filtra paquetes que entren por la interfaz E0 de Yosemite, que es la primera interfaz del router por la que entran los paquetes enviados por Sam. El tema de tener paquetes "enrutados alrededor" de listas de acceso en interfaces serie es tenido en cuenta con el emplazamiento en la única interfaz Ethernet de Yosemite. También, el filtrado ordenado por el segundo requisito (para deshabilitar el acceso de los hosts LAN de Seville a Yosemite) se consigue con la segunda sentencia access-list. Parando el flujo de paquetes desde la subred LAN de Yosemite a la subred LAN de Seville se detiene efectivamente la comunicación entre las dos subredes. Alternativamente, la lógica opuesta podría ser configurada en Seville.

Avances en la gestión de la configuración de las ACLs

Ahora que se han entendido los conceptos centrales de las ACLs IP del IOS, esta sección examina un par de mejoras en el soporte de las ACLs por parte del IOS: ACLs con nombre y números de secuencia ACL. Aunque ambas características son útiles e importantes, ninguna añade ninguna función de lo que un router puede o no filtrar, en comparación con las ACLs numeradas ya tratadas en este capítulo. En cambio, las ACLs con nombre y los números de secuencia ACL proporcionan al ingeniero opciones de configuración que hacen más fácil recordar los nombres de ACL y más fácil editar las ACLs ya existentes cuando es necesario modificar una ACL.

Listas de acceso IP con nombre

Las ACLs con nombre, introducidas en la versión 11.2 del IOS, pueden utilizarse para hacer coincidir los mismos paquetes, con los mismos parámetros, que pueden hacerse coincidir con las ACLs IP estándares y extendidas. Las ACLs IP con nombre tienen algunas diferencias que facilitan su uso. La diferencia más obvia es que el IOS identifica las ACLs con nombre utilizando nombres en lugar de números (y es más fácil recordar nombres).

Además de utilizar nombres memorizables más fácilmente, la otra gran ventaja de las ACLs con nombre respecto a las ACLs numeradas, en el momento en que fueron introducidas en el IOS, fue que se podía borrar líneas individuales de una lista de acceso IP con nombre. A lo largo de la historia de las ACLs IP numeradas y el comando global ip access-list, hasta la introducción del IOS 12.3, es que no era posible borrar una única línea en una ACL numerada. Por ejemplo, si ya se configuró el comando ip access-list 101 permit tcp any any eq 80, y entonces se ejecuta el comando no ip access-list 101 permit tcp any any eq 80, ¡se podría borrar la ACL 101 entera! La ventaja de la introducción de las ACLs con nombre es que se puede ejecutar un comando que elimine líneas individuales de una ACL.

Nota

Con el IOS 12.3, Cisco expande el IOS para permitir borrar líneas individuales en las ACLs numeradas, haciendo que el IOS soporte la edición tanto de las ACLs numeradas como de las ACLs con nombre. Estos detalles se explican en la siguiente sección.

La sintaxis de configuración es muy similar entre las listas de acceso IP numeradas y con nombre. Los elementos que pueden coincidir con una lista de acceso IP estándar numerada son idénticos a los elementos que pueden coincidir con una lista de acceso IP estándar con nombre. Igualmente, los elementos son idénticos en las listas de acceso IP extendidas numeradas y con nombre.

Existen dos importantes diferencias de configuración entre el viejo estilo de las ACLs numeradas y el nuevo de las listas de acceso con nombre. Una diferencia clave es que las listas de acceso con nombre utilizan un comando global que coloca al usuario en un submodo de lista de acceso IP con nombre, en el cual se configura la coincidencia y la lógica de permitir/denegar. La otra diferencia clave es que cuando una sentencia de coincidencia con nombre se borra, sólo esta sentencia se borra.

El Ejemplo 6.9 muestra un ejemplo que utiliza ACLs IP con nombre. Muestra cómo ha cambiado el indicador de comandos, mostrando que el usuario ha entrado en el modo de configuración de ACL. También muestra las partes pertinentes de la salida de un comando show running-configuration. Finaliza con un ejemplo de cómo se puede borrar una línea individual en una ACL con nombre.

Ejemplo 6.9. Configuración de las listas de acceso con nombre.

```
conf t
Enter configuration commands, one per line. End with Ctrl-Z.
Router(config)#ip access-list extended barney
Router(config-ext-nacl)#permit tcp host 10.1.1.2 eq www any
Router(config-ext-nacl)#deny udp host 10.1.1.1 10.1.2.0 0.0.0.255
Router(config-ext-nacl)#deny ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
! La siguiente sentencia es errónea a propósito para que se pueda ver
! el proceso de modificación de la lista.
Router(config-ext-nacl)#deny ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255

Router(config-ext-nacl)#deny ip host 10.1.1.130 host 10.1.3.2
Router(config-ext-nacl)#deny ip host 10.1.1.28 host 10.1.3.2
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#interface serial1
Router(config-if)#ip access-group barney out
Router(config-if)#^Z
Router#show running-config
Building configuration...
Current configuration:
.
```

(continúa)

Ejemplo 6.9. Configuración de las listas de acceso con nombre *(continuación).*

```
. (Se omiten las sentencias sin importancia)
.
interface serial 1
 ip access-group barney out
!
ip access-list extended barney
 permit tcp host 10.1.1.2 eq www any
 deny   udp host 10.1.1.1 10.1.2.0 0.0.0.255
 deny   ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
 deny   ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255
 deny   ip host 10.1.1.130 host 10.1.3.2
 deny   ip host 10.1.1.28 host 10.1.3.2
 permit ip any any
Router#conf t
Enter configuration commands, one per line. End with Ctrl-Z.
Router(config)#ip access-list extended barney
Router(config-ext-nacl)#no deny ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255
Router(config-ext-nacl)#^Z
Router#show access-list

Extended IP access list barney
    10 permit tcp host 10.1.1.2 eq www any
    20 deny udp host 10.1.1.1 10.1.2.0 0.0.0.255
    30 deny ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
    50 deny ip host 10.1.1.130 host 10.1.3.2
    60 deny ip host 10.1.1.28 host 10.1.3.2
    70 permit ip any any
```

El Ejemplo 6.9 comienza con la creación de una ACL llamada barney. El comando ip access-list extended barney crea la ACL, llamándola barney y colocando al usuario en el modo de configuración de ACL. Este comando también le dice al IOS que barney es una ACL extendida. Después, siete sentencias diferentes permit y deny definen la lógica de coincidencia y acción a tomar ante una coincidencia. Los comandos permit y deny utilizan la misma sintaxis que los comandos numerados access-list, comenzando con las palabras clave deny y permit. En este ejemplo, se añade un comentario justo antes del comando que se borra después en el ejemplo.

La salida del comando show running-config muestra la configuración de la ACL con nombre antes de borrar una única entrada. Después, el comando no deny ip... borra una única entrada de la ACL. Observe que la salida del comando show running-config muestra ahora la ACL, con seis comandos permit y deny en lugar de siete.

Edición de ACLs empleando números de secuencia

Las ACLs numeradas existen en el IOS desde los primeros días de los routers de Cisco. Desde su creación, hasta la versión 12.2 del IOS, la única forma de editar una ACL numera-

da existente (por ejemplo, para simplemente borrar una línea de la ACL) era borrar la ACL entera y entonces reconfigurarla. Además, siendo un inconveniente para el ingeniero, este proceso también causa algunos desafortunados efectos colaterales. Cuando se borra una ACL, es importante deshabilitar la ACL en todas las interfaces, y después borrarla, reconfigurarla, y habilitarla en la interfaz. Si no, durante el proceso de reconfiguración, antes de que todas las sentencias sean reconfiguradas, la ACL no realizará todas las validaciones que debe, a veces causando problemas, o exponiendo a la red a varios ataques.

Como se ha mencionado en la sección anterior, el soporte original de las ACLs con nombre por parte del IOS, introducido en el IOS 11.2, resuelve algunos de los problemas de edición. Los comandos originales para las ACLs con nombre permitían al ingeniero borrar una línea de una ACL, como se ha mostrado en la sección anterior en el Ejemplo 6.9. Sin embargo, los comandos de configuración no permitían al usuario insertar un nuevo comando permit o deny en la lista. Todos los comandos nuevos se añadían al final de la ACL.

Con el IOS 12.3, Cisco introduce más opciones de configuración para las ACLs; opciones que se aplican tanto a las ACLs IP con nombre como a las numeradas. Estas opciones se aprovechan de un número de secuencia que se añade a cada sentencia ACL permit o deny, con los números representando la secuencia de las sentencias en la ACL. Los números de secuencia de ACL proporcionan características para ambas, las ACLs numeradas y con nombre:

- Una sentencia permit o deny individual de ACL se puede borrar haciendo referencia al número de secuencia, sin borrar el resto de la ACL.
- Nuevamente los comandos permit y deny añadidos se pueden configurar con un número de secuencia, dictando la localización de las sentencias en la ACL.
- Nuevamente los comandos permit y deny añadidos se pueden configurar **sin** un número de secuencia, de modo que el IOS crea un número de secuencia y coloca el comando al final de la ACL.

Para aprovechar la habilidad de borrar e insertar líneas en una ACL, las ACLs numeradas y con nombre deben utilizar el mismo estilo de configuración global utilizado en las ACLs con nombre. La única diferencia en la sintaxis es si se usa un número o un nombre. El Ejemplo 6.10 muestra la configuración de una ACL IP estándar numerada, usando este estilo de configuración alternativo. El ejemplo muestra la potencia de los números de secuencia ACL para editar. En este ejemplo, ocurre lo siguiente:

Paso 1 Se configura la ACL numerada 24, usando este nuevo estilo de configuración, con tres comandos permit.

Paso 2 El comando show ip access-list muestra los tres comandos "permitir", con los números de secuencia 10, 20 y 30.

Paso 3 El ingeniero borra sólo el segundo comando permit, usando el subcomando ACL no 20, que simplemente hace referencia al número de secuencia 20.

Paso 4 El comando show ip access-list confirma que la ACL ahora tiene sólo dos líneas (números de secuencia 10 y 30).

Paso 5 El ingeniero añade un comando permit al comienzo de la ACL, usando el subcomando ACL 5 deny 10.1.1.1.

Paso 6 El comando show ip access-list de nuevo confirma los cambios, esta vez mostrando los tres comandos permit, con los números de secuencias 5, 10 y 30.

NOTA

Para este ejemplo, observe que el usuario no abandona el modo de configuración, sino que utiliza el comando do para decir al IOS que ejecute el comando EXEC show ip access-list desde el modo de configuración.

Ejemplo 6.10. Editando ACLs usando números de secuencia.

```
! Paso 1: Se configura la tercera línea de la ACL IP estándar numerada.
R1#configure terminal
Enter configuration commands, one per line. End with Ctrl-Z.
R1(config)#ip access-list standard 24
R1(config-std-nacl)#permit 10.1.1.0 0.0.0.255
R1(config-std-nacl)#permit 10.1.2.0 0.0.0.255
R1(config-std-nacl)#permit 10.1.3.0 0.0.0.255
! Paso 2: Mostrar el contenido de la ACL, sin dejar el modo de configuración.
R1(config-std-nacl)#do show ip access-list 24
Standard IP access list 24
    10 permit 10.1.1.0, wildcard bits 0.0.0.255
    20 permit 10.1.2.0, wildcard bits 0.0.0.255
    30 permit 10.1.3.0, wildcard bits 0.0.0.255
! Paso 3: Todavía en el modo de configuración de la ACL 24, se borra la línea
! con el número de secuencia 20.
R1(config-std-nacl)#no 20
! Paso 4: Mostrar de nuevo el contenido de la ACL, sin dejar el modo de
! configuración. Observe que ya no se muestra la línea número 20.
R1(config-std-nacl)#do show ip access-list 24
Standard IP access list 24
    10 permit 10.1.1.0, wildcard bits 0.0.0.255
    30 permit 10.1.3.0, wildcard bits 0.0.0.255
! Paso 5: Insertar una nueva primera línea en la ACL.
R1(config-std-nacl)#5 deny 10.1.1.1
! Paso 6: Mostrar el contenido de la ACL una última vez, con la nueva sentencia
! (número de secuencia 5) como la primera.
R1(config-std-nacl)#do show ip access-list 24
Standard IP access list 24
     5 deny 10.1.1.1
    10 permit 10.1.1.0, wildcard bits 0.0.0.255
    30 permit 10.1.3.0, wildcard bits 0.0.0.255
```

De forma interesante, las ACLs numeradas pueden ser configuradas con el nuevo estilo de configuración, como se muestra en el Ejemplo 6.10, o con el viejo estilo de configuración, usando los comandos de configuración global, como se muestra en los primeros ejemplos de este capítulo. De hecho, se pueden usar ambos estilos de configuración en una

única ACL. Sin embargo, no importa qué estilo de configuración se utilice, la salida del comando show running-config muestra todavía los comandos de configuración en el viejo estilo. El Ejemplo 6.11 demuestra estos hechos, siguiendo donde acabó el Ejemplo 6.10, con los siguientes pasos adicionales:

Paso 7 El ingeniero lista la configuración (show running-config), que muestra los comandos de configuración con el estilo antiguo, incluso aunque la ACL se creara con los comandos del nuevo estilo.

Paso 8 El ingeniero añade una nueva sentencia al final de la ACL, usando el comando de configuración global access-list 24 permit 10.1.4.0 0.0.0.255 del viejo estilo.

Paso 9 El comando show ip access-list confirma que el comando del viejo estilo access-list de los pasos anteriores sigue la regla de añadirse al final de la ACL.

Paso 10 El ingeniero muestra la configuración para confirmar que las partes de la ACL 24 configurada con los comandos del nuevo y viejo estilo se muestran todos en el mismo viejo estilo de ACL (show running-config).

Ejemplo 6.11. Añadiendo y mostrando una configuración de ACL numerada.

```
! Paso 7: Un trozo de la configuración de la ACL 24.
R1#show running-config
! The only lines shown are the lines from ACL 24
access-list 24 deny 10.1.1.1
access-list 24 permit 10.1.1.0 0.0.0.255
access-list 24 permit 10.1.3.0 0.0.0.255

! Paso 8: Añadiendo un nuevo comando access-list 24
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 24 permit 10.1.4.0 0.0.0.255
R1(config)#^Z
! Paso 9: Mostrando de nuevo el contenido de la ACL, con los números
! de secuencia. Observe que se ha asignado automáticamente un número de secuencia
! a la nueva sentencia.
R1#show ip access-list 24
Standard IP access list 24
    5 deny 10.1.1.1
    10 permit 10.1.1.0, wildcard bits 0.0.0.255
    30 permit 10.1.3.0, wildcard bits 0.0.0.255
    40 permit 10.1.4.0, wildcard bits 0.0.0.255
!
! Paso 10: La configuración de la ACL numerada permanece en comandos
! de configuración del viejo estilo.
R1#show running-config
! Las únicas líneas mostradas son las líneas de la ACL 24
access-list 24 deny 10.1.1.1
access-list 24 permit 10.1.1.0 0.0.0.255
access-list 24 permit 10.1.3.0 0.0.0.255
access-list 24 permit 10.1.4.0 0.0.0.255
```

Temas varios sobre las ACLs

Esta corta sección cubre un par de pequeños temas: cómo filtrar tráfico Telnet y SSH usando ACLs, y algunas líneas generales de implementación.

Control de acceso por Telnet y SSH empleando ACLs

Un ingeniero puede controlar el acceso remoto a un router utilizando ACLs que buscan puertos bien conocidos usados por Telnet (23) y SSH (22). Sin embargo, para hacer el trabajo habilitando ACLs en las interfaces usando el subcomando de interfaz ip access-group, la ACL podría necesitar verificar todas las direcciones IP de los routers, además de los puertos Telnet y SSH. Si se configuran nuevas interfaces, la ACL podría necesitar ser actualizada.

El IOS proporciona una opción más fácil para proteger el acceso hacia y desde los puertos de línea de terminal virtual (vty, *virtual terminal line*). Los usuarios Telnet y SSH se conectan a líneas vty en un router; por tanto, para proteger este acceso, se puede aplicar una ACL IP a las líneas vty. Se pueden utilizar ACLs para impedir que los hosts IP puedan hacer telnet al router, y también se pueden limitar los hosts a los que un usuario del router puede hacer telnet.

Por ejemplo, imagine que sólo los hosts de la subred 10.1.1.0/24 se suponen capaces de hacer telnet a cualquier router de Cisco de una red. En tal caso, la configuración mostrada en el Ejemplo 6.12 se puede utilizar en cada router para denegar el acceso desde las direcciones IP que no son de esta subred.

Ejemplo 6.12. Control de acceso de vty usando el comando **access-class**.

```
line vty 0 4
 login
 password cisco
 access-class 3 in
!
! El siguiente comando es un comando global
 access-list 3 permit 10.1.1.0 0.0.0.255
```

El comando access-class se refiere a la lógica de coincidencia en access-list 3. La palabra clave in se refiere a las conexiones Telnet a este router; en otras palabras, la gente haciendo telnet a este router. Como se ha configurado, la ACL 3 verifica la dirección IP de origen de los paquetes para las conexiones Telnet entrantes.

Si se utilizara el comando access-class 3 out, se podría tener que comprobar no sólo los Telnet salientes, sino también la dirección IP de destino de los paquetes. Filtrar las conexio-

nes Telnet y SSH salientes, comprobando la dirección IP de origen, que por definición debe ser una de las direcciones IP de interfaz en este router, realmente no tendría ningún sentido. Para filtrar sesiones Telnet salientes, tiene más sentido filtrar basándose en la dirección IP de destino. Por tanto, el uso del comando access-class 3 out, concretamente la palabra clave out, es uno de los casos raros en los que una ACL IP estándar realmente mira la dirección IP de destino y no la de origen.

Consideraciones de la implementación de una ACL

En redes IP de producción, la creación de ACLs IP, la resolución de problemas y las actualizaciones pueden consumir una gran cantidad de tiempo y esfuerzo. El examen ICND2 no tiene muchas preguntas sobre las cosas a tener en cuenta cuando se implementan ACLs IP en redes reales, pero trata unos pocos temas, que se discuten en esta sección.

Cisco hace las siguientes recomendaciones generales en los cursos en los cuales se basan los exámenes CCNA:

Tema clave

- Crear las ACLs usando un editor de texto fuera del router, y copiar y pegar las configuraciones en el router. (Incluso con la posibilidad de borrar e insertar líneas en una ACL, la creación de los comandos en un editor podría ser aún un proceso más fácil.)
- Colocar las ACLs extendidas lo más cerca posible del origen de los paquetes a descartar para descartar los paquetes rápidamente.
- Colocar las ACLs estándares tan cerca del destino de los paquetes como sea posible, porque las ACLs estándares a menudo descartan paquetes que no se desea que sean descartados si se colocan cerca del origen.
- Colocar las sentencias más específicas al principio de la ACL.
- Deshabilitar una ACL de su interfaz (usando el comando no ip access-group) antes de hacer cambios en la ACL.

La primera sugerencia dice que se creen las ACLs fuera del router usando un editor. Así, si se cometen errores al teclear, se pueden corregir en el editor. Esta sugerencia ya no es tan importante como lo era en las versiones del IOS anteriores a la 12.3, ya que esta última soporta los números de línea de ACL y el borrado e inserción de líneas sencillas en una ACL, como se ha descrito antes, en la sección "Edición de ACLs empleando número de secuencia".

Nota

Si se crean todas las ACLs en un editor de texto, puede ser útil comenzar cada fichero con el comando no access-list *número*, seguido de los comandos de configuración en la ACL. Entonces, cada vez que se edite el fichero de texto para modificar la ACL, todo lo que tiene que hacer es copiar y pegar el contenido entero del fichero, con la primera línea borrando el contenido entero de la ACL existente, y el resto de sentencias recreando la nueva ACL.

Los puntos segundo y tercero tienen que ver con el concepto de dónde colocar las ACLs. Si se intenta filtrar un paquete, filtrando lo más cerca del origen del paquete, significa que el

paquete consume menos ancho de banda en la red, lo que parece ser más eficiente, y lo es. Por tanto, Cisco sugiere colocar las ACLs extendidas lo más cerca posible del origen.

Sin embargo, Cisco también sugiere, al menos en los cursos relativos a CCNA, colocar las ACLs estándares cerca del destino. ¿Por qué no cerca del origen de los paquetes? Bien, ya que las ACLs estándares sólo miran en la dirección IP de origen, tienden a filtrar más de lo que realmente se desea filtrar cuando se colocan cerca del origen. Por ejemplo, imagine que Fred y Barney están separados por cuatro routers. Si se filtra el tráfico que Barney envía a Fred en el primer router, Barney no puede alcanzar cualquier host cerca de los otros tres routers. Por tanto, el curso ICND2 de Cisco hace una recomendación general de localizar las ACLs estándares lo más próximas al destino para evitar filtrar tráfico que no pensaba filtrar.

Colocando los parámetros de coincidencia más específicos al principio de cada lista, es menos probable que se cometan errores en la ACL. Por ejemplo, imagine que se tiene una sentencia que permite todo el tráfico desde 10.1.1.1 a 10.2.2.2, destinado al puerto 80 (la web), y otra sentencia que deniega todos los otros paquetes originados en la subred 10.1.1.0/24. Ambas sentencias podrían coincidir con paquetes enviados por el host 10.1.1.1 a un servidor web en 10.2.2.2, pero probablemente se quería hacer coincidir la sentencia más específica (permitir) primero. En general, colocando la sentencia más específica primero tiende a asegurar que no se nos olvida nada.

Finalmente, Cisco recomienda que se deshabiliten las ACLs en las interfaces antes de cambiar las sentencias de la lista. Afortunadamente, si se tiene una ACL IP habilitada en una interfaz con el comando `ip access-group`, y se borra la ACL entera, el IOS no filtra ningún paquete. (¡Lo que no era siempre el caso en las primeras versiones de IOS!) Incluso, tan pronto como se añade un comando a la ACL, el IOS comienza el filtrado de paquetes. Supongamos que la ACL 101 está habilitada en S0 para los paquetes de salida. Se borra la lista 101; por tanto, todos los paquetes están autorizados a circular. Después se ejecuta el comando `access-list 101`. Tan pronto como se pulsa Intro, la lista existe, y el router filtra todos los paquetes que salen por S0 basándose en la lista de una línea. Si se desea añadir una ACL más larga, puede que temporalmente se estén filtrando paquetes que no se desea filtrar. Por tanto, la mejor manera es deshabilitar la lista de la interfaz, hacer los cambios en la lista, y después rehabilitarla en la interfaz.

Listas de acceso reflexivas

Las ACLs reflexivas, también llamadas filtrado de sesión IP, proporcionan una manera de prevenir una clase de ataques de seguridad al permitir de forma individual cada sesión TCP o UDP. Para hacer esto, el router reacciona cuando ve el primer paquete de una nueva sesión entre dos hosts. Reacciona al paquete añadiendo una sentencia permitir a la ACL, permitiendo el tráfico de la sesión basándose en la dirección IP de origen y de destino y el puerto TCP/UDP.

La Figura 6.9 muestra un caso clásico en el cual las ACLs tradicionales crean un agujero de seguridad, pero las ACLs reflexivas podrían tapar el agujero. La mayoría de las empresas desean permitir a los usuarios el uso de navegadores web para conectar con servidores web basados en Internet. Una ACL extendida tradicional podría permitir el tráfico

permitiendo tráfico hacia y desde cualesquiera dos direcciones IP, pero con la verificación adicional en el puerto TCP utilizado por HTTP (puerto 80). En este caso, la figura muestra una ACL que comprueba el puerto de origen 80 para los paquetes que entran en la empresa, lo que significa que los paquetes proceden de un servidor web.

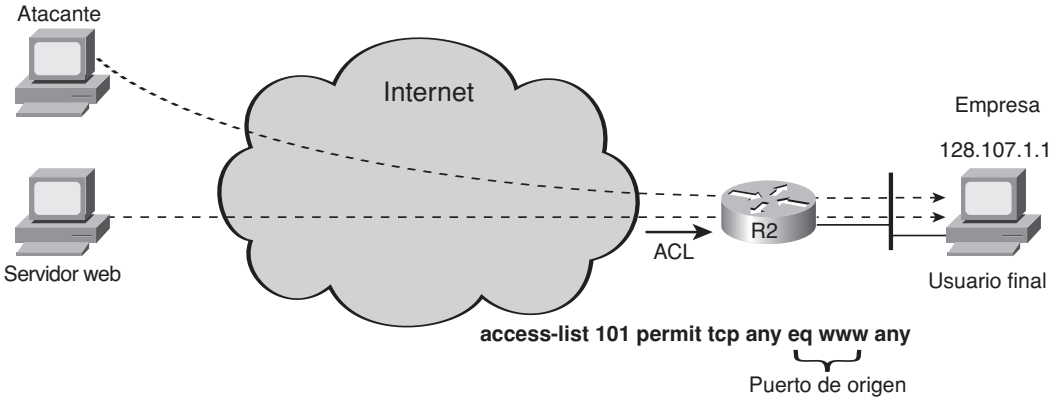


Figura 6.9. La necesidad de ACLs reflexivas.

La ACL utilizada en R2 filtra todo el tráfico entrante excepto el tráfico procedente de los servidores web. Esto permite al servidor basado en Internet de la izquierda enviar paquetes al usuario de la Empresa de la derecha. Sin embargo, también permite al atacante enviar paquetes, con puerto de origen 80, con el router permitiendo el paso de paquetes. Aunque estos paquetes pueden no ser parte de una conexión TCP existente, algunos ataques conocidos pueden hacer uso de estos paquetes; desde un simple ataque de Denegación de servicio por inundación de paquetes en la Empresa, hasta aprovecharse de fallos conocidos del sistema operativo.

Las ACLs reflexivas permiten a los usuarios legítimos enviar y recibir paquetes a través del router, mientras se descartan los paquetes de otros hosts, como los paquetes del atacante de la Figura 6.9. Con las ACLs reflexivas, cuando el usuario de la Empresa crea una nueva sesión, el router advierte la nueva sesión y registra las direcciones IP de origen y de destino y los puertos utilizados en esa sesión. La ACL reflexiva de R2 podría no permitir en ella todo el tráfico del puerto 80. En cambio, podría permitir sólo los paquetes cuyas direcciones y puertos coincidan con el paquete original. Por ejemplo, si el PC de la derecha comienza una sesión con el servidor web legítimo, puerto de origen 1030, R2 podría permitir paquetes desde Internet si tienen las siguientes características: dirección IP de origen 64.100.2.2, dirección IP de destino 128.107.1.1, puerto de origen 80, puerto de destino 1030. Como resultado, sólo se permiten a través del router los paquetes de la sesión legítima, y los paquetes enviados por el atacante se descartan.

Las ACLs reflexivas necesitan una configuración adicional, así como el uso de configuración de ACLs extendidas con nombre.

ACLs dinámicas

Las ACLs dinámicas solucionan un problema diferente que tampoco se soluciona fácilmente utilizando ACLs tradicionales. Imagine un conjunto de servidores que necesitan ser accedidos por un conjunto pequeño de usuarios. Con las ACLs, se pueden hacer coincidir las direcciones IP de los hosts utilizados por los usuarios. Sin embargo, si el usuario toma prestado otro PC, u obtiene otra dirección usando DHCP, o utiliza su portátil de casa, etcétera, el usuario legítimo tiene ahora una dirección IP diferente. Por tanto, una ACL tradicional podría tener que ser editada para permitir cada nueva dirección IP. Con el tiempo, mantener una ACL que verifique todas estas direcciones IP podría ser muy pesado. Además, introduciría la posibilidad de agujeros de seguridad cuando los hosts de otros usuarios comiencen a utilizar una de las viejas direcciones IP.

Las ACLs dinámicas, también denominadas *Lock-and-Key Security* (Seguridad bloqueo-y-clave), solucionan este problema tratando la ACL como un proceso de autenticación de usuarios. En lugar de comenzar tratando de conectar con el servidor, el usuario debe hacer primero telnet a un router. El router le pregunta la combinación nombre de usuario/contraseña. Si es auténtico, el router cambia dinámicamente su ACL, permitiendo tráfico desde la dirección IP del host que acaba de enviar los paquetes de autenticación. Después de un periodo de inactividad, el router borra la entrada dinámica en la ACL, cerrando el potencial agujero de seguridad. La Figura 6.10 muestra la idea.

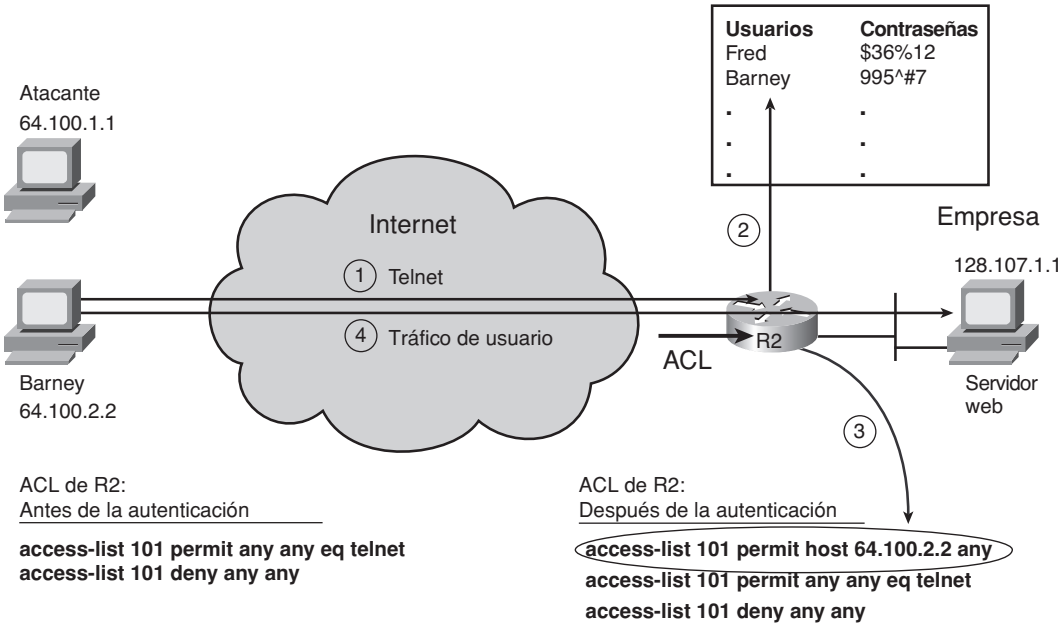


Figura 6.10. ACLs dinámicas.

El proceso mostrado en la figura comienza con el router denegando todo el tráfico excepto Telnet. (Aunque la figura muestra una ACL que permite hacer telnet a cualquier dirección IP, en la práctica, el tráfico Telnet sólo se necesita permitir en una dirección IP del router). Para iniciar el proceso, ocurren los siguientes pasos:

Paso 1 El usuario conecta con el router usando Telnet.

Paso 2 El usuario proporciona un nombre de usuario/clave, que el router compara con una lista, autenticando al usuario.

Paso 3 Después de la autenticación, el router añade dinámicamente una entrada al comienzo de la ACL, permitiendo tráfico originado en el host autenticado.

Paso 4 Los paquetes enviados por el host permitido pasan a través del router hacia el servidor.

ACLs basadas en tiempos

El término ACL basada en el tiempo se refiere a una característica de las ACLs IP normales (numeradas o con nombre) según la cual se puede añadir una restricción temporal a los comandos de configuración. En algunos casos, esto podría ser útil para coincidir con paquetes en una ACL, pero sólo cada cierto tiempo en el día, o incluso en unos días concretos de la semana. Las ACLs basadas en el tiempo permiten añadir restricciones temporales, con el IOS manteniendo o eliminando las sentencias de la ACL en el momento apropiado del día.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 6.8 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 6.8. Temas clave del Capítulo 6.

Tema clave	Descripción	Número de página
Figura 6.2	Diagrama mostrando cuándo un router examina los paquetes con ACLs de entrada y de salida.	228
Lista	Cuatro pasos que describen cómo un router procesa una ACL multilínea.	230
Tabla 6.2	Explicación de ejemplos de máscaras *wildcard* y su significado.	231
Lista	Atajo para encontrar valores en el comando access-list para coincidir con un número de subred, dado el número de subred y la máscara de subred.	232
Lista	Atajo para interpretar la dirección y la máscara *wildcard* en un comando access-list como un número de subred y una máscara.	232-233
Lista	Lista de planificación y verificación de ACLs.	234
Tabla 6.3	Lista de campos del paquete IP que se pueden comprobar mediante las ACLs estándares y extendidas.	239
Lista	Consejos para la coincidencia de puertos TCP y UDP usando ACLs IP.	240-241
Figura 6.6	Muestra un paquete con el puerto de origen y de destino, con la correspondiente localización del parámetro de puerto de origen en el comando access-list.	242
Lista	Tres elementos en los que difieren las ACLs IP estándares y extendidas.	243

(continúa)

Tabla 6.8. Temas clave del Capítulo 6 *(continuación).*

Tema clave	Descripción	Número de página
Tabla 6.7	Lista de operadores que pueden ser utilizados cuando se comparan números de puerto en los comandos access-list extendidos.	244
Lista	Características de las ACLs numeradas y con nombre proporcionadas por los números de secuencia de ACL.	250
Lista	Lista de sugerencias de buenas prácticas en las ACLs acordes con los cursos autorizados CCNA de Cisco.	254

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD) o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas completas para validar su trabajo.

Lectura de los escenarios del Apéndice F

El apéndice F, "Escenarios adicionales", contiene cinco escenarios detallados que le ofrecen la oportunidad de analizar diferentes diseños, problemas y salidas de comandos. También muestran cómo se interrelacionan los conceptos de varios capítulos. El Escenario 3 se centra en las ACLs IP, incluyendo prácticas sobre cómo elegir las máscaras *wildcard* ACL para coincidir con todos los hosts de una única subred.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe sus respuestas en el glosario:

ACL dinámica, ACL reflexiva, lista de acceso estándar, lista de acceso extendida, lista de acceso con nombre, máscara *wildcard*.

Referencias de comandos

Aunque no necesariamente debe memorizar la información de las tablas de esta sección, ésta incluye una referencia de los comandos de configuración y EXEC utilizados en este capítulo. En la práctica, debería memorizar los comandos como un efecto colateral de leer el capítulo y hacer todas las actividades de esta sección de preparación del examen. Para ver hasta qué punto se han memorizado los comandos como efecto secundario de su estudio, lea las descripciones que hay en el lado derecho e intente recordar el comando que debe aparecer a la izquierda.

Tabla 6.9. Comandos de configuración del Capítulo 6.

Comando	Descripción
access-list *número-lista-acceso* {deny | permit} *origen* [*wildcard-origen*] [log]	Comando global para las listas de acceso estándares numeradas. Usa un número entre 1 y 99 ó 1300 y 1999, incluidos.
access-list *número-lista-acceso* {deny | permit} *protocolo origen wildcard-origen destino wildcard-destino* [log]	Comando global para las listas de acceso extendidas numeradas. Utiliza un número entre 100 y 199 ó 2000 y 2699, incluidos.
access-list *numero-lista-acceso* {deny | permit} tcp *origen wildcard-origen* [*operador* [*puerto*]] *destino wildcard-destino* [*operador* [*puerto*]] [log]	Una versión del comando access-list con parámetros específicos de TCP.
access-list *número-lista-acceso* remark *texto*	Define un comentario que ayuda a recordar lo que se supone que hace la ACL.
ip access-group {*número* | *nombre* [in | out]}	Subcomando de interfaz que habilita las listas de acceso.
access-class *número* | *nombre* [in | out]	Subcomando de línea que habilita tanto las listas de acceso estándares como las extendidas.
ip access-list {standard | extended} *nombre*	Comando global para configurar una ACL con nombre estándar o extendida y entra en el modo de configuración de ACL.
{deny | permit} *origen* [*wildcard-origen*] [log]	Subcomando de modo ACL para configurar los detalles de la coincidencia y la acción para una ACL estándar con nombre.

(continúa)

Tabla 6.9. Comandos de configuración del Capítulo 6 *(continuación)*.

Comando	Descripción
{deny | permit} *protocolo origen wildcard-origen destino wildcard-destino* [log]	Subcomando de modo de ACL para configurar los detalles de coincidencia y la acción para una ACL extendida con nombre.
{deny | permit} tcp *origen wildcard-origen* [*operador* [*puerto*]] *destino wildcard-destino* [*operador* [*puerto*]] [log]	Subcomando de modo ACL para configurar los detalles de coincidencia y la acción para una ACL con nombre que coincida con segmentos TCP.
remark *texto*	Subcomando de modo ACL para configurar una descripción de una ACL con nombre.

Tabla 6.10. Comandos EXEC del Capítulo 6.

Comando	Descripción
show ip interface [*tipo número*]	Incluye una referencia a las listas de acceso habilitadas en la interfaz.
show access-lists [*número-lista-acceso* | *nombre-lista-acceso*]	Muestra detalles de las listas de acceso configuradas para todos los protocolos.
show ip access-list [*número-lista-acceso* | *nombre-lista-acceso*]	Muestra las listas de acceso IP.

Este capítulo trata los siguientes temas:

Los comandos ping y traceroute: Esta sección explica cómo funcionan los comandos ping y traceroute, junto con los matices de cómo se pueden usar para mejorar la resolución de problemas de enrutamiento.

Resolución de problemas en el proceso de envío de paquetes: Esta sección examina el proceso de envío de paquetes, centrándose en el enrutamiento host y en cómo los routers enrutan paquetes. También se tratan temas relacionados con el envío de paquetes en ambas direcciones entre dos hosts.

Herramientas y pautas para la resolución de problemas: Esta sección trata una amplia variedad de temas que tienen algún efecto en el proceso de envío de paquetes. Incluye algunas pautas de varios comandos y conceptos que pueden ayudar en el proceso de resolución de problemas.

CAPÍTULO 7

Resolución de problemas de enrutamiento IP

Este capítulo de resolución de problemas tiene varios objetivos. Primero, se explican varias herramientas y funciones no tratadas en los Capítulos 4 hasta 6; concretamente, herramientas que pueden ser de gran ayuda cuando se analizan problemas. Este capítulo revisa los conceptos de los otros tres capítulos de la Parte II, "Enrutamiento IP". Aúna los conceptos y sugiere un proceso para resolver los problemas de enrutamiento, así como ejemplos de cómo utilizarlo. La segunda mitad del capítulo se centra en una serie de pautas de resolución de problemas para muchos de los temas tratados en los Capítulos 4 a 6.

Cuestionario "Ponga a prueba sus conocimientos"

Los capítulos de resolución de problemas de este libro aúnan conceptos de otros capítulos, incluyendo algunos capítulos del libro *CCENT/CCNA ICND1*. Estos capítulos muestran cómo acercarse a algunas de las preguntas más desafiantes de los exámenes CCNA. Por tanto, es útil leer estos capítulos sin importar su nivel de conocimiento actual. Por estas razones, el capítulo de resolución de problemas no incluye un cuestionario "Ponga a prueba sus conocimientos". Sin embargo, si se siente particularmente confiado con las características de las resolución de problemas de enrutamiento IP tratadas en este libro y en el libro *CCENT/CCNA ICND1*, puede pasar directamente a la sección "Ejercicios para la preparación del examen", cerca del final de este capítulo.

Temas fundamentales

Este capítulo se centra en la resolución de problemas del proceso de enrutamiento IP. Para este fin, comienza con una sección acerca de dos importantes herramientas de resolución de problemas: ping y traceroute. A continuación de esto, el capítulo examina el proce-

so de encaminamiento IP desde una perspectiva de resolución de problemas, en concreto centrándose en cómo aislar los problemas de enrutamiento para identificar la causa raíz del problema. La sección final trata una amplia variedad de pequeños temas, que pueden ser útiles cuando se resuelvan problemas de enrutamiento IP.

Nota

Este capítulo, y el Capítulo 15 del libro *CCENT/CCNA ICND1*, explican detalles de cómo resolver problemas del proceso de enrutamiento IP. El enrutamiento IP es de importancia vital en los exámenes ICND1 e ICND2, así como en el examen CCNA; por tanto, existe un solapamiento entre los exámenes, lo que requiere cierto solapamiento en los libros. Sin embargo, este capítulo trata muchos temas que van más allá de los detalles necesarios para el examen ICND1. Para estar completamente preparado, lea el capítulo entero, pero puede omitir aquellas partes del capítulo que le parezcan repetitivas respecto al libro ICND1.

Los comandos ping y traceroute

Esta sección examina un proceso sugerido de resolución de problemas de enrutamiento IP; en otras palabras, el proceso del plano de datos de cómo las computadoras y los routers envían paquetes IP. Para este fin, esta sección primero examina un conjunto de herramientas y protocolos útiles, en concreto, ICMP, ping y traceroute. Después de esto, el texto sugiere un buen proceso general de resolución de problemas para problemas de IP, con unos pocos ejemplos para mostrar cómo utilizarlos.

Protocolo de mensajes de control en Internet (ICMP)

TCP/IP incluye ICMP, un protocolo designado para ayudar a gestionar y controlar el funcionamiento de una red TCP/IP. El protocolo ICMP proporciona una amplia variedad de información sobre el estado operacional de la red. **Mensajes de control** es la parte más descriptiva del nombre. ICMP ayuda al control y a la gestión de IP definiendo un conjunto de mensajes y procedimientos acerca del funcionamiento de IP. Por tanto, ICMP es considerado parte de la capa de red de TCP/IP. Debido a que ICMP ayuda al control de IP, puede proporcionar información útil para la resolución de problemas. De hecho, los mensajes de ICMP se sitúan dentro del paquete IP, sin cabecera de capa de transporte; así, ICMP es realmente una extensión de la capa de red de TCP/IP.

La RFC 792 define ICMP. El siguiente extracto de la RFC 792 describe bien el protocolo:

> Ocasionalmente un gateway (router) o host de destino comunicará con un host de origen; por ejemplo, para informar de un error en el procesamiento de un datagrama. Para tal propósito, se utiliza este protocolo, el Protocolo de mensajes de con-

trol en Internet (ICMP). ICMP utiliza el soporte básico de IP como si fuera un protocolo de capa superior; no obstante, ICMP es realmente una parte integral de IP y debe estar implementado en todos los módulos IP.

ICMP define varios tipos diferentes de mensajes para cumplir con sus variadas tareas, como se resume en la Tabla 7.1.

Tabla 7.1. Tipos de mensajes ICMP.

Mensaje	Descripción
Destino inalcanzable	Le dice a la computadora de origen que hay un problema en la entrega del paquete.
Tiempo excedido	El tiempo que tiene un paquete para ser entregado ha finalizado; por tanto, el paquete ha de ser descartado.
Redirigir	El router envía este mensaje cuando recibe un paquete para el cual otro router tiene una ruta mejor. El mensaje le dice al remitente que utilice la ruta mejor.
Petición de eco, Respuesta de eco	Usados por el comando ping para verificar la conectividad.

El comando ping, y la petición de eco y la respuesta de eco ICMP

El comando ping utiliza los mensajes de petición y respuesta de eco de ICMP. De hecho, cuando la gente dice que envía un paquete ping, realmente significa que envían una Petición de eco ICMP. Estos dos mensajes son de alguna forma autoexplicativos. La Petición de eco simplemente significa que el host al que va dirigida debería responder al paquete. La Respuesta de eco es el tipo de mensaje ICMP que será utilizado en la respuesta. La Petición de eco incluye algunos datos que se pueden especificar en el comando ping; cualquier dato que se envía en la Petición de eco es devuelto en la Respuesta de eco.

El comando ping en sí mismo proporciona varias formas creativas de utilizar las Peticiones y Respuestas de eco. Por ejemplo, el comando ping permite especificar la longitud, así como las direcciones de origen y destino, y también establecer otros campos en la cabecera IP. El Capítulo 4, "Enrutamiento IP: rutas estática y conectadas", muestra un ejemplo del comando ping extendido que muestra las distintas opciones.

El mensaje de destino inalcanzable de ICMP

Este libro se centra en IP. Pero desde un punto de vista más amplio, el objetivo del conjunto entero de protocolos TCP/IP es entregar datos desde la aplicación remitente a la apli-

cación receptora. Los hosts y los routers envían mensajes de destino inalcanzable de ICMP al host emisor cuando este host o router no entrega los datos completamente a la aplicación del host de destino.

Para ayudar en la resolución de problemas, el mensaje inalcanzable de ICMP incluye cinco funciones (códigos) inalcanzables que identifican tanto la identidad de la causa como el paquete que no puede ser entregado. Los cinco tipos de códigos pertenecen directamente a una característica de IP, TCP o UDP.

Por ejemplo, la interred mostrada en la Figura 7.1 puede utilizarse para entender mejor algunos códigos Inalcanzables. Se asume que Fred está tratando de conectar con un servidor web, llamado Web. (Web utiliza HTTP, que a su vez utiliza TCP como protocolo de nivel de transporte). Tres de los códigos Inalcanzable de ICMP serán posiblemente utilizados por los routers A y B. Los otros dos códigos se utilizan por el servidor web. Estos códigos de ICMP se envían a Fred como un resultado del paquete originalmente enviado por Fred.

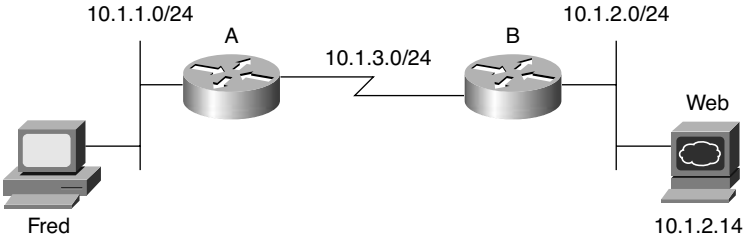


Figura 7.1. Red de ejemplo para explicar los códigos inalcanzables de ICMP.

La Tabla 7.2 resume los códigos inalcanzables más comunes de ICMP. Después de la tabla, el texto explica cómo cada código ICMP puede ser necesario en la red mostrada en la Figura 7.1.

La siguiente lista explica cada código de la Tabla 7.2 con mayor detalle utilizando la red de la Figura 7.1 como un ejemplo:

- **Red inalcanzable:** El Router A utiliza este código si no tiene una ruta por la que remitir el paquete. En este caso, el router necesita enrutar el paquete a la subred 10.1.2.0/24. Si no puede, el Router A envía a Fred el mensaje de destino inalcanzable de ICMP con el código "red inalcanzable" en respuesta al paquete de Fred destinado a 10.1.2.14.
- **Host inalcanzable:** Este código implica que el único host de destino no está disponible. Si el Router A tiene una ruta a 10.1.2.0/24, el paquete es entregado al Router B. Si la interfaz LAN del Router B está funcionando, B también tiene una ruta conectada a 10.1.2.0/24; por tanto, B trata de invocar ARP y aprender la dirección MAC del servidor web. Sin embargo, si el servidor web no está funcionando, el Router B no recibirá la respuesta ARP del servidor web. El Router B envía a Fred el mensaje de destino inalcanzable de ICMP con el código "host de red inalcanzable,"

Tabla 7.2. Códigos inalcanzables de ICMP.

Código inalcanzable	Cuándo se utiliza	Quién lo envía típicamente
Red inalcanzable	No hay conincidencia en la tabla de enrutamiento para el destino del paquete.	Router
Host inalcanzable	El paquete puede ser enrutado a un router conectado a la subred de destino, pero el host no está respondiendo.	Router
No se puede fragmentar	El paquete tiene activado el bit No Fragmentar, y un router debe fragmentar para enviar el paquete.	Router
Protocolo inalcanzable	El paquete es entregado al host de destino, pero el protocolo de capa de transporte no está disponible en este host.	Host
Puerto inalcanzable	El paquete es entregado al host de destino, pero ninguna aplicación tiene abierto el puerto de destino.	Host

lo que significa que B tiene una ruta pero no puede enviar el paquete directamente a 10.1.2.14.

- **No se puede fragmentar:** Este código es el último de los tres códigos inalcanzables ICMP que un router puede enviar. La fragmentación define el proceso en el cual un router necesita fragmentar un paquete, pero la interfaz de salida permite sólo paquetes que son más pequeños que el paquete. El router está autorizado a fragmentar el paquete en piezas, pero en la cabecera del paquete IP puede establecerse el bit de "No fragmentar". En este caso, si el Router A o B necesita fragmentar el paquete, pero el bit No fragmentar está establecido en la cabecera IP, el router descarta el paquete y envía a Fred un mensaje de destino inalcanzable de ICMP con el código "No fragmentar."
- **Protocolo inalcanzable:** Si el paquete llega correctamente al servidor web, aún son posibles otros dos códigos inalcanzables. Uno implica que el protocolo por encima de IP, típicamente TCP o UDP, no se está ejecutando en este host. Esto es bastante improbable, ya que la mayoría de los sistemas operativos que utilizan TCP/IP usan un único paquete software que proporciona las funciones de IP, TCP y UDP. Pero si el host recibe el paquete IP y TCP o UDP no está disponible, el host servidor web envía a Fred el mensaje de destino inalcanzable de ICMP con el código "protocolo inalcanzable" en respuesta al paquete de Fred destinado a 10.1.2.14.
- **Puerto inalcanzable:** Este valor del campo de código es más probable hoy en día. Si el servidor (la computadora) está encendida y funcionando, pero el software del ser-

vidor web no se está ejecutando, el paquete puede ser obtenido por el servidor pero no será entregado al software del servidor web. En efecto, el servidor no está escuchando en el puerto bien conocido del protocolo de esta aplicación. Por tanto, el host 10.1.2.14 envía a Fred el mensaje de destino inalcanzable con el código "puerto inalcanzable" en respuesta al paquete de Fred destinado a 10.1.2.14.

Nota

La mayoría de las políticas de seguridad hoy en día filtran algunos de estos mensajes inalcanzables para ayudar en la seguridad de la red.

El comando ping muestra varias respuestas que en algunos casos implican que será recibido un mensaje inalcanzable. La Tabla 7.3 especifica los códigos inalcanzables que puede mostrar el comando ping del software IOS de Cisco.

Tabla 7.3. Códigos que el comando **ping** recibe en respuesta a sus peticiones de eco de ICMP.

Código del comando ping	Descripción
!	Respuesta de eco ICMP recibida.
.	No se ha recibido nada antes de expirar el comando ping.
U	Recibido (destino) inalcanzable de ICMP.
N	Recibido (red/subred) inalcanzable de ICMP.
M	Recibido mensaje No se puede fragmentar de ICMP.
?	Recibido un paquete desconocido.

El mensaje Redirigir de ICMP

El mensaje Redirigir de ICMP proporciona un medio por el cual los routers pueden decir a los hosts que utilicen otro router como gateway predeterminado para ciertas direcciones de destino. La mayoría de los hosts utilizan el concepto de una dirección IP de router predeterminado, enviando paquetes destinados a las subredes por su router predeterminado. Sin embargo, si varios routers conectan con la misma subred, el gateway predeterminado de un host puede no ser la mejor ruta para esa subred hacia la cual enviar paquetes enviados a algunos destinos. El gateway predeterminado puede reconocer que una ruta distinta es una mejor opción. Entonces puede enviar un mensaje redirigir de ICMP al host para decirle que envíe los paquetes para esa dirección de destino por esta ruta diferente.

Por ejemplo, en la Figura 7.2, el PC utiliza el Router B como su router predeterminado. Sin embargo, la ruta del Router A a la subred 10.1.4.0 es una ruta mejor. (Se asume el uso de una

máscara 255.255.255.0 en cada subred de la Figura 7.2.) El PC envía un paquete al Router B (Paso 1 en la Figura 7.2). El Router B entonces reenvía el paquete basándose en su propia tabla de enrutamiento (Paso 2); esa ruta es a través del Router A, que tiene una mejor ruta. Finalmente, el Router B envía el mensaje redirigir de ICMP al PC (Paso 3), diciéndole que reenvíe los futuros paquetes para 10.1.4.0 al Router A. Irónicamente, el host puede ignorar la redirección y seguir enviando los paquetes al Router B, pero en este ejemplo, el PC cree en el mensaje de redirección, enviando sus próximos paquetes (Paso 4) directamente al Router A.

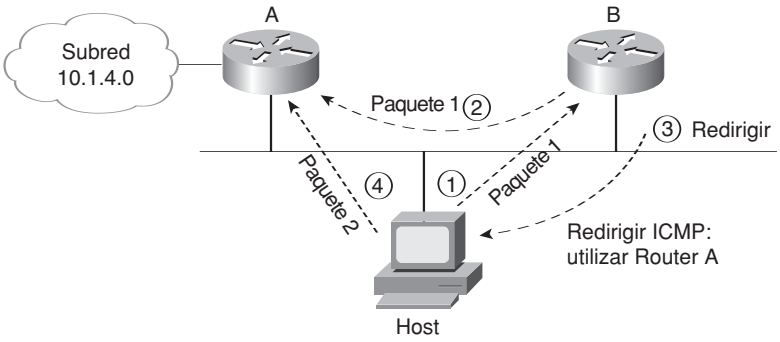


Figura 7.2. Redirigir ICMP.

El mensaje de Tiempo excedido de ICMP

El mensaje de Tiempo excedido notifica a un host cuando un paquete que él envió ha sido descartado por "tiempo agotado". Los paquetes no están realmente cronometrados, pero para prevenir que sean reenviados por siempre cuando hay un bucle de enrutamiento, la cabecera IP utiliza un campo Tiempo de existencia (TTL, *Time to Live*). Los routers decrementan el TTL en 1 cada vez que reenvían un paquete; si un router decrementa el TTL a 0, desecha el paquete. Esto evita que los paquetes viajen por siempre por la red. La Figura 7.3 muestra este proceso básico.

Como se puede ver en la figura, el router que descarta el paquete también envía un mensaje de Tiempo excedido ICMP, con un campo de código de "tiempo excedido" al host que envía el paquete. De esta forma, el remitente conoce que el paquete no fue entregado. Obtener un mensaje de Tiempo excedido también puede ayudar cuando se solucionan problemas en una red. Afortunadamente, no se dan demasiados de estos; de lo contrario, se tendrían problemas de enrutamiento.

El comando traceroute

El comando ping es una utilidad potentísima que puede utilizarse para contestar a la pregunta "¿Funciona la ruta de aquí hasta allí?" El comando traceroute proporciona una

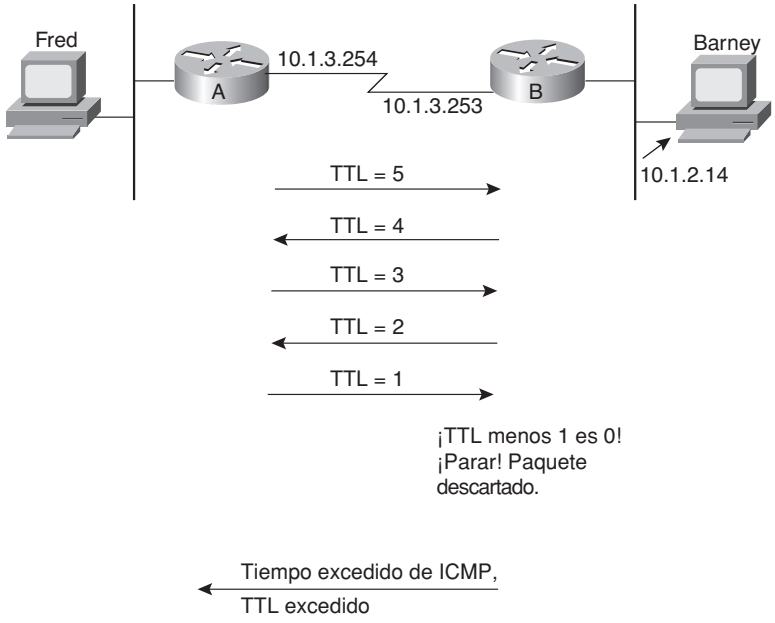


Figura 7.3. TTL decrementado en 0.

herramienta de resolución de problemas indiscutiblemente mejor porque no sólo puede determinar si la ruta funciona, sino que proporciona la dirección IP de cada router en la ruta. Si la ruta no está funcionando, traceroute puede identificar los mejores lugares para comenzar con la resolución de un problema.

El comando traceroute del IOS utiliza el mensaje de Tiempo excedido y el campo TTL de IP para identificar cada router sucesivo en una ruta. El comando traceroute envía un conjunto de mensajes con el valor TTL incrementándose, comenzando con 1. El comando traceroute espera que estos mensajes sean descartados cuando los routers decrementen el TTL a 0, devolviendo mensajes de Tiempo excedido al comando traceroute. La dirección IP de origen de los mensajes de Tiempo excedido identifica las rutas que descartan los mensajes, que se pueden entonces mostrar con el comando traceroute.

Para ver cómo funciona este comando, considere el primer conjunto de paquetes (tres paquetes de forma predeterminada) enviados por el comando traceroute. Los paquetes son paquetes IP, con una capa de transporte UDP, y con el TTL establecido a 1. Cuando los paquetes llegan al siguiente router, el router decrementa el TTL a 0 en cada paquete, descartando el paquete y devolviendo un mensaje de Tiempo excedido al host que envió el paquete descartado. El comando traceroute mira la dirección IP de origen del primer router en el paquete de Tiempo excedido recibido.

A continuación, el comando traceroute envía otro conjunto de tres paquetes IP, esta vez con TTL = 2. El primer router decrementa el TTL a 1 y reenvía los paquetes, y el segundo router decrementa el TTL a 0 y descarta los paquetes. Este segundo router devuelve men-

sajes de Tiempo excedido al router donde el comando traceroute se utilizó, y el comando traceroute ahora conoce al segundo router de la ruta.

El comando traceroute conoce cuándo llegan al host de destino los paquetes de test porque el host devuelve un mensaje ICMP de Puerto inalcanzable. Los paquetes originales enviados por el comando traceroute del IOS utilizan un número de puerto UDP que es muy improbable que se esté utilizando en el host de destino; tan pronto como el TTL es lo suficientemente largo para permitir que el paquete llegue al host de destino, el host notifica que no hay ninguna aplicación escuchando en ese puerto UDP. Por tanto, el host de destino devuelve un mensaje de Puerto inalcanzable, que le dice al comando traceroute que se ha encontrado la ruta completa, y el comando puede parar.

La Figura 7.4 muestra un ejemplo, pero sólo con uno de los tres mensajes en cada TTL (para reducir el desorden). El Router A utiliza el comando traceroute tratando de encontrar la ruta a Barney. El Ejemplo 7.1 muestra este comando traceroute en el Router A, con mensajes de depuración del Router B, mostrando los tres mensajes resultantes de Tiempo excedido.

El comando traceroute lista la dirección IP del Router B en la primera línea y la dirección IP del host de destino en la segunda. Observe que muestra la dirección IP del lado izquierdo del Router B. B contesta con el mensaje de Tiempo excedido, usando la dirección IP de la interfaz de salida de B como la dirección de origen en ese paquete. Como resultado, el comando traceroute lista esta dirección IP. Si la dirección es conocida para un servidor de DNS, o si está en la tabla de nombres de host del Router A, el comando puede mostrar el nombre del host en vez de la dirección IP.

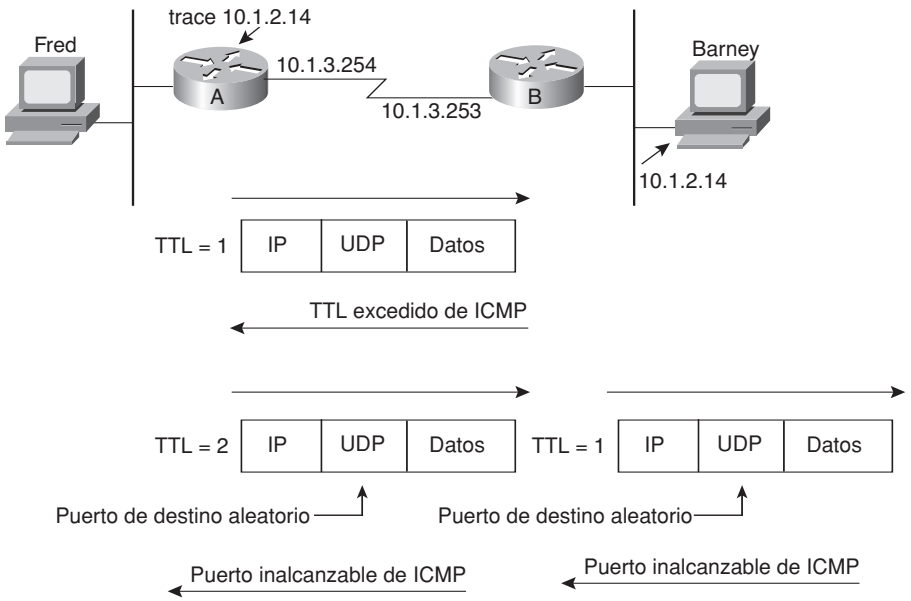


Figura 7.4. Comando **traceroute** del software IOS de Cisco: mensajes generados.

Ejemplo 7.1. **Debug** de ICMP en el Router B cuando se ejecuta el comando **traceroute** en el Router A.

```
RouterA#traceroute 10.1.2.14

Type escape sequence to abort.
Tracing the route to 10.1.2.14

  1 10.1.3.253 8 msec 4 msec 4 msec
  2 10.1.2.14 12 msec 8 msec 4 msec
RouterA#
```

```
! Ahora en el Router B
! La siguiente salida es la reacción al comando traceroute en A
RouterB#debug ip icmp
RouterB#
ICMP: time exceeded (time to live) sent to 10.1.3.254 (dest was 10.1.2.14)
ICMP: time exceeded (time to live) sent to 10.1.3.254 (dest was 10.1.2.14)
ICMP: time exceeded (time to live) sent to 10.1.3.254 (dest was 10.1.2.14)
```

Similar al comando ping extendido como se describió en la sección "El comando ping extendido" del Capítulo 4, la versión extendida del comando traceroute hace un trabajo mucho mejor de simulación de paquetes enviados por un host de usuario final, más concretamente testeando rutas inversas. Por ejemplo, en el Ejemplo 7.1, el comando traceroute de A utiliza la dirección IP 10.1.3.254 de A como la dirección de origen de los paquetes enviados, porque A utiliza la interfaz con dirección 10.1.3.254 para enviar paquetes generados por el comando traceroute. Por tanto, el comando traceroute del Ejemplo 7.1 testea la ruta de reenvío hacia 10.1.2.14 y la ruta inversa hacia 10.1.3.254. El comando traceroute extendido puede utilizarse para testear una ruta inversa más apropiada, tal como la ruta hacia la subred LAN del lado izquierdo del Router A. El Ejemplo 7.2, más adelante en este capítulo, muestra un ejemplo del comando traceroute extendido.

Nota

El comando tracert en los sistemas operativos Microsoft funciona de forma muy parecida al comando traceroute de IOS. No obstante, es importante observar que el comando tracert de Microsoft envía Peticiones de Eco de ICMP y no utiliza UDP. Por tanto, las ACLs de IP podrían provocar que traceroute de IOS falle mientras que tracert de Microsoft funcione y viceversa.

Resolución de problemas en el proceso de envío de paquetes

La resolución de problemas del proceso de enrutamiento IP es una de las tareas más complejas que realizan los ingenieros de redes. Como es habitual, el uso de una metodolo-

gía estructurada puede ayudar. El Capítulo 4 en concreto, así como los Capítulos 5 y 6, han explicado ya mucho acerca de la primera parte principal del proceso de resolución de problemas; lo que podría pasar en una red. Esta sección se centra en el segundo paso principal: el aislamiento del problema. (Para una referencia más general de las técnicas de resolución de problemas, consulte el Capítulo 3, "Resolución de problemas con la conmutación LAN").

Nota

Este capítulo difiere cualquier detalle de la resolución de problemas de los protocolos de enrutamiento hasta el Capítulo 11, "Resolución de problemas en los protocolos de enrutamiento".

Aislamiento de problemas de enrutamiento IP relacionados con los hosts

El proceso de resolución de problemas perfilado en este capítulo separa los pasos de resolución de problemas; una parte para los hosts, y otra para los routers. Esencialmente, para cualquier problema en el cual dos hosts no pueden comunicarse, la primera parte de este proceso de resolución de problemas examina el problema que podría influir sobre la capacidad del host para enviar paquetes hacia y desde su respectivo gateway predeterminado. La segunda parte aísla problemas relativos a la forma en que los routers envían paquetes.

La siguiente lista esboza los pasos de la resolución de problemas centrándose en verificar la conectividad del host con el primer router:

Paso 1 Verificar la habilidad del host para enviar paquetes en su propia subred. Bien ejecutando el comando ping a la dirección IP del gateway predeterminado del host desde el propio host, o haciendo un ping a la dirección IP del host desde el gateway predeterminado. Si falla el ping, hacer lo siguiente:

- **a.** Asegurar que la interfaz del router utilizada como gateway predeterminado está en un estado "*up* y *up*".
- **b.** Verificar la dirección IP del host de origen y la máscara establecida comparándolas con la interfaz del router utilizada como gateway predeterminado. Asegurarse de que ambas coinciden en el número y máscara de subred, y por tanto coinciden en el rango de direcciones válidas en la subred.
- **c.** Si el router utiliza el *trunking* VLAN, solucionar cualquier problema de configuración del troncal, asegurándose que el router está configurado para soportar la misma VLAN a la que pertenece el host.
- **d.** Si los otros pasos no encuentran una solución, investigar los problemas de capa 1/2 con la LAN, como se trata en el Capítulo 3. Por ejemplo, buscar VLANs no definidas.

Paso 2 Verificar la configuración del gateway predeterminado en el host haciendo ping a otra dirección IP de interfaz del router predeterminado. O, desde el router predeterminado, utilizar un ping extendido de la dirección IP del host con la dirección de origen de otra de las interfaces del router.

Por ejemplo, en la Figura 7.5, el síntoma del problema puede ser que PC1 no puede acceder al servidor web de PC4. Para verificar la habilidad de PC1 de enviar paquetes en su subred local, PC1 puede utilizar el comando ping 10.1.1.1 para verificar la conectividad del router predeterminado con su misma subred. O el ingeniero podría simplemente hacer ping 10.1.1.10 desde R1 (Paso 1). La ejecución de ping en otro sitio funciona bien, porque ambas ubicaciones de ping necesitan que un paquete sea enviado en cada dirección. Si el ping falla, el aislamiento del problema debe destapar las dos áreas del problema especificadas en los Pasos 1A, 1B y 1C. Si no, es probable que el problema sea un problema de capa 1 ó 2, como los tratados en el Capítulo 3.

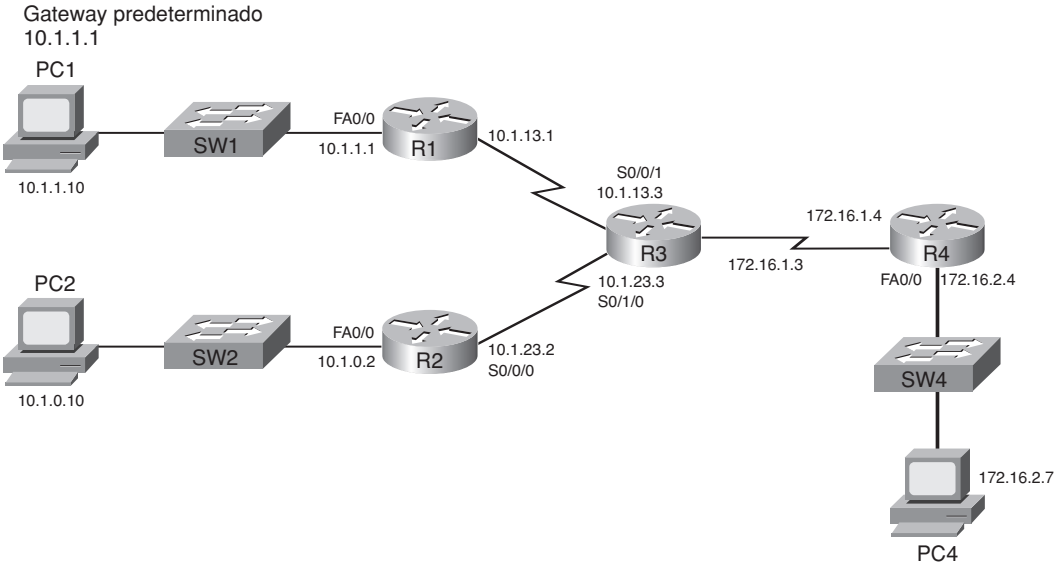


Figura 7.5. Red de ejemplo para escenarios de resolución de problemas.

El Paso 2 recuerda un concepto de resolución de problemas a menudo pasado por alto para verificar que la configuración del gateway predeterminado está funcionando. Ninguna opción de ping especificada en el Paso 1 requiere que el host utilice su configuración de gateway predeterminado, porque la dirección de origen y de destino en cada paquete están en la misma subred. El Paso 2 fuerza al host a enviar un paquete a una dirección IP en otra subred; por tanto, testea la configuración de gateway predeterminado del host. También, al hacer ping a una dirección IP del gateway (router) predeterminado, en lugar de a alguna dirección IP de host situado más allá, este paso elimina mucha complejidad en el enrutamiento IP de prueba. En cambio, la atención se centra en si funciona o no la configuración de gateway predetermi-

nado del host. Por ejemplo, en la Figura 7.5, un comando ping 10.1.13.1 con PC1 impone a PC1 el uso de su configuración de gateway predeterminado porque 10.1.13.1 no está en la subred de PC1 (10.1.1.0/24). Pero la dirección IP es la del router R1, que elimina gran parte del resto de la red como posible causa de que el ping falle.

Aislamiento de problemas de enrutamiento IP relacionados con los routers

Cuando el proceso de aislamiento de problemas en los hosts finaliza, y todos los pings funcionan, en los hosts emisor y receptor podría aún existir algún problema de enrutamiento IP entre el primero y el último router tanto en la ruta de envío como en la inversa entre los dos hosts. La siguiente lista muestra los procesos de resolución de problemas con el gateway/router predeterminado del host de origen, confiando en el comando traceroute en el router. (Observe que el comando equivalente del host, tal como tracert en los sistemas operativos Microsoft, también se puede utilizar.)

Nota

Aunque la siguiente lista se puede usar como referencia, es bastante larga. No se hunda en los detalles, sino que lea los ejemplos de uso que siguen a esta lista, que clarificarán muchos de los pasos. Como es habitual, no necesita memorizar los procesos de resolución de problemas explicados aquí. Simplemente son herramientas de aprendizaje que le ayudarán a desarrollar sus habilidades.

Paso 3 Testear la conectividad al host de destino con el comando traceroute extendido en el gateway predeterminado del host, usando la interfaz del router conectada al host de origen para la dirección IP de origen de los paquetes. Si el comando se completa con éxito:

- No existen problemas de enrutamiento en las direcciones de la ruta de envío ni en la inversa.
- Si el tráfico del usuario final todavía no funciona (aunque traceroute funcione), solucionar los problemas en cualquier ACL en cada interfaz en cada router de la ruta, en ambas direcciones.

Paso 4 Si el comando traceroute del Paso 3 no se completa, verificar la **ruta predeterminada** como sigue:

a. Hacer telnet al último router analizado (el último router listado en el comando traceroute).

b. Encontrar la ruta del router que coincide con la dirección IP de destino que se utilizó en el comando traceroute original (show ip route, show ip route *dirección-ip*).

c. Si no se encuentra ninguna ruta coincidente, investigar por qué la ruta esperada no aparece. Normalmente existe un problema con el protocolo de

enrutamiento o un error de configuración de la ruta estática. También podría estar relacionado con la pérdida de una ruta conectada.

d. Si se encuentra una ruta coincidente, y la ruta es una ruta predeterminada, confirmar que se utilizará basándose en la configuración del comando ip classless/no ip classless.

e. Si se encuentra una ruta, hacer ping a la dirección IP del siguiente salto especificada en la ruta. O, si la ruta es una ruta conectada, ping a la verdadera dirección IP de destino.

- Si el ping falla, investigar los problemas de capa 2 entre este router y la dirección IP a la que se hizo ping, e investigar posibles problemas de ACL.
- Si el ping funciona, investigar problemas de ACL.

f. Si se encuentra una ruta coincidente, y no se encuentran otros problemas, confirmar que la ruta no está apuntando equivocadamente en una dirección errónea.

Paso 5 Si el Paso 4 no identifica un problema en la ruta de envío, verificar la **ruta inversa**:

- Si la ruta de envío en el último router analizado se refiere a otro router como el router de siguiente salto, repetir los subpasos del Paso 3 en este router de siguiente salto. Analizar la ruta inversa; la ruta a cada dirección IP de origen utilizada por el comando traceroute que falla.
- Si la ruta de envío en el último router analizado se refiere a una subred conectada, verificar la configuración IP de destino del host. En concreto, confirmar la configuración para la dirección IP, máscara y gateway predeterminado.

Por ejemplo, si PC1 no puede comunicar con PC4 en la Figura 7.5, y los hosts pueden ambos comunicar a través de sus respectivos gateways predeterminados, el Paso 3 del proceso de aislamiento de problemas orientados al router podría comenzar con un traceroute 172.16.2.7, usando la dirección IP de Fa0/0 de R1 (10.1.1.1) como la dirección IP de origen. Si este comando traceroute muestra a 10.1.13.3 como la última dirección IP en la salida del comando, en vez de terminar, se podría entonces comenzar el Paso 4, el cual examina la ruta de envío de R3 hacia 172.16.2.7. Si el análisis del Paso 4 no descubre el problema, el Paso 5 podría entonces pasar al router de siguiente salto, R4 en este cado, y examinar la ruta inversa de R4; esta ruta regresa a la dirección de origen 10.1.1.1.

A continuación, se muestran dos escenarios separados que muestran cómo se utilizan estos pasos de resolución de problemas para aislar algunos problemas de ejemplo.

Escenario de resolución de problemas nº 1: problemas con la ruta de envío

Este primer ejemplo del proceso de resolución de problemas de router utiliza la misma internetwork mostrada en la Figura 7.5. En este caso, PC1 no puede utilizar un navegador web para conectar al servicio web ejecutándose en PC4. Antes de investigar más allá, PC1 no puede hacer ping a 172.16.2.7 (PC4). El Ejemplo 7.2 muestra los comandos utilizados en

R1 y R4 para los Pasos 1 y 2 orientados al host, así como un inicio del Paso 3 orientado al router.

Ejemplo 7.2. Escenario 1 de resolución de problemas: Pasos 1 y 2 y parte del Paso 3.

```
R1#ping 10.1.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.13.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
Packet sent with a source address of 10.1.13.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#
```

```
! Ahora se repite la prueba en R4
R4#ping 172.16.2.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R4#show ip interface brief
Interface         IP-Address     OK? Method Status                    Protocol
FastEthernet0/0   172.16.2.4     YES manual administratively down     down
FastEthernet0/1   172.16.1.4     YES manual up                        up
Serial0/0/0       unassigned     YES unset  administratively down     down
Serial0/0/1       unassigned     YES unset  administratively down     down
Serial0/1/0       unassigned     YES unset  administratively down     down
```

Los pings estándares y extendidos en R1 al comienzo del ejemplo realizan esencialmente los Pasos 1 y 2, los pasos orientados al host, para confirmar que PC1 parece estar funcionando bien. Sin embargo, el ejemplo posterior muestra que R4 no puede alcanzar PC4

porque la interfaz LAN de R4 ha sido cerrada, como se muestra al final del ejemplo. Aunque este escenario puede parecer un poco simple, proporciona un buen punto de inicio para solucionar un problema.

Para tener una visión más completa del proceso de resolución de problemas, considere a continuación este mismo escenario, con el mismo problema raíz, pero ahora no se tiene acceso al router R4. Por tanto, se pueden realizar sólo los Pasos 1 y 2 para PC1, que funcionan, pero no se pueden hacer esos mismos pasos para PC4 desde R4. Así, el Ejemplo 7.3 avanza al Paso 3 y 4. El comienzo del ejemplo muestra el Paso 3, donde R1 utiliza traceroute 172.16.2.7, con una dirección IP de origen de 10.1.1.1. Este comando no finaliza, y hace referencia a 10.1.13.3 (R3) como el último router. El Paso 4 continúa entonces comprobando cómo R3 enruta paquetes destinados a 172.16.2.7.

Ejemplo 7.3. Escenario 1 de resolución de problemas: Paso 4.

```
R1#traceroute
Protocol [ip]:
Target IP address: 172.16.2.7
Source address: 10.1.1.1
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 172.16.2.7

  1 10.1.13.3 0 msec 4 msec 0 msec
  2 10.1.13.3 !H * !H
! Observe arriba que el comando finaliza por sí mismo, pero no lista el
! host de destino 172.16.2.7
R3#show ip route 172.16.2.7
% Subnet not in table
R3#show ip route
Codes:  C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 1 subnets
C        172.16.1.0 is directly connected, FastEthernet0/0
      10.0.0.0/24 is subnetted, 4 subnets
```

(continúa)

Ejemplo 7.3. Escenario 1 de resolución de problemas: Paso 4 *(continuación)*.

```
C       10.1.13.0 is directly connected, Serial0/0/1
R       10.1.1.0 [120/1] via 10.1.13.1, 00:00:04, Serial0/0/1
R       10.1.0.0 [120/1] via 10.1.23.2, 00:00:01, Serial0/1/0
C       10.1.23.0 is directly connected, Serial0/1/0
```

El comando traceroute extendido al comienzo del ejemplo muestra la salida identificando R3 (10.1.13.3) como el último dispositivo listado en la salida del comando (Paso 3). El Paso 4 entonces procede con un examen de la ruta de envío de R3 hacia la dirección IP 172.16.2.7. El comando show ip route 172.16.2.7 va directamente al grano. El mensaje "la subred no está en la tabla" significa que R3 no tiene una ruta coincidente con la dirección 172.16.2.7. Si la pregunta no proporciona acceso a un simulador, sólo la salida del comando show ip route, podría ser necesario examinar las rutas para determinar que ninguna de ellas se refiere a un rango de direcciones que incluya a 172.16.2.7.

A veces los procesos de aislamiento de problemas apuntan a una ruta perdida; el siguiente paso es determinar cómo el router podría haber aprendido esta ruta. En este caso, R3 podría haber usado RIP-2 para aprender la ruta. Por tanto, los siguientes pasos podrían ser solucionar cualquier problema con el protocolo de enrutamiento dinámico.

La causa raíz de este problema no ha cambiado (R4 ha cerrado su interfaz Fa0/0) pero los síntomas son en cierta forma interesantes. Debido a que la interfaz está cerrada, R4 no publica rutas para la subred 172.16.2.0/24 a R3. Sin embargo, R3 publica una ruta resumida para la subred 172.16.0.0/16 a R1 y R2; por tanto, R1 y R2, debido a la configuración predeterminada de autoresumen de RIP-2, pueden reenviar paquetes destinados a 172.16.2.7 por R3. Como resultado, el comando traceroute en R1 puede reenviar paquetes a R3.

Escenario de resolución de problemas nº 2: problema con la ruta inversa

Este ejemplo utiliza el mismo diagrama de red mostrado en la Figura 7.5, siendo cierta todavía toda la información mostrada en la misma. Sin embargo, los detalles mencionados en la sección previa pueden haber cambiado (en concreto el problema que existe para hacer el ejemplo más interesante). Así, afrontar este segundo ejemplo confiando sólo en la figura como cierta.

En este escenario, PC1 de nuevo no puede hacer ping a 172.16.2.7 (PC4). El gateway predeterminado de host verifica lo sugerido en los Pasos 1 y 2 que de nuevo funciona en PC1, pero las pruebas no pueden realizarse en la dirección inversa, porque el ingeniero no puede acceder a PC4 o al router R4. Por tanto, el Ejemplo 7.4 muestra el proceso de resolución de problemas sugerido en el Paso 3, mostrando el resultado del comando traceroute extendido en R1. Observe que el comando ni siquiera lista la dirección IP de R3 10.1.13.3 en este caso. Por tanto, el resto del Ejemplo 7.4 muestra la investigación en los subpasos específicos del Paso 4.

Ejemplo 7.4. Escenario 2 de resolución de problemas: Pasos 3 y 4.

```
R1#traceroute ip 172.16.2.7 source fa0/0

Type escape sequence to abort.
Tracing the route to 172.16.2.7

  1 * * *
  2 * * *
  3 *
R1#show ip route 172.16.2.7
Routing entry for 172.16.0.0/16
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 10.1.13.3 on Serial0/1/0, 00:00:05 ago
  Routing Descriptor Blocks:
  * 10.1.13.3, from 10.1.13.3, 00:00:05 ago, via Serial0/1/0
      Route metric is 1, traffic share count is 1

R1#ping 10.1.13.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.13.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#show ip access-lists
```

```
! A continuación cambiamos al router R3
R3#show ip access-lists
R3#
```

El ejemplo comienza mostrando parte del proceso del Paso 3, con el comando traceroute mostrando únicamente líneas de asteriscos. Esto significa que el comando no identifica correctamente ni siquiera el primer router en la ruta.

Ya en el Paso 4, la siguiente lista esboza los subpasos de dicho paso aplicados a este ejemplo:

Paso 4a El ejemplo puede comenzar con un Telnet a R1; por tanto, no es necesario un trabajo extra.

Paso 4b El siguiente comando, show ip route 172.16.2.7, muestra que R1 tiene una ruta no predeterminada para la red 172.16.0.0, apuntado hacia R3 (10.1.13.3) como el siguiente salto.

Paso 4c Este paso no es aplicable en este caso, porque se encontró una ruta coincidente en el Paso 4B.

Paso 4d Este paso no es aplicable en este caso, porque la ruta coincidente no es una ruta hacia 0.0.0.0/0 (la ruta predeterminada).

Paso 4e El siguiente comando listado, ping 10.1.13.3, verifica la habilidad de R1 de enviar paquetes por el enlace al router de siguiente salto identificado en el Paso 4B. El ping funciona.

Paso 4f En ambos, R1 y el router de siguiente salto (R3), el comando show ip access-lists confirma que ningún router tiene ninguna ACL IP configurada.

Debido a que se han pasado todos los pasos para examinar la ruta de envío, el proceso avanza al Paso 5. El comando traceroute original en el Ejemplo 7.4 utiliza la dirección IP de la interfaz Fa0/0 de R1, 10.1.1.1, como la dirección IP de origen. Para el Paso 5, el proceso comienza en R3 con un análisis de la ruta inversa de R3 para alcanzar 10.1.1.1. Examine la salida del Ejemplo 7.5, y busque algún problema antes de leer la explicación que sigue al ejemplo.

Ejemplo 7.5. Escenario 2 de resolución de problemas: Paso 5.

```
! El siguiente comando muestra la ruta coincidente, para la subred 10.1.1.0/26,
! con el siguiente salto 10.1.23.2.
R3#show ip route 10.1.1.1
Routing entry for 10.1.1.0/26
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 10.1.23.2
      Route metric is 0, traffic share count is 1

! El siguiente comando muestra las subredes solapadas - 10.1.1.0/26 y 10.1.1.0/24.
R3#show ip route
Codes:  C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 2 subnets
C        172.16.1.0 is directly connected, FastEthernet0/0
R        172.16.2.0 [120/1] via 172.16.1.4, 00:00:18, FastEthernet0/0
      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C        10.1.13.0/24 is directly connected, Serial0/0/1
S        10.1.1.0/26 [1/0] via 10.1.23.2
R        10.1.1.0/24 [120/1] via 10.1.13.1, 00:00:10, Serial0/0/1
R        10.1.0.0/24 [120/1] via 10.1.23.2, 00:00:11, Serial0/1/0
C        10.1.23.0/24 is directly connected, Serial0/1/0
```

R3 tiene una ruta estática configurada incorrectamente para la subred 10.1.1.0/26. Esta subred incluye el rango de direcciones 10.1.1.0–10.1.1.63, que incluye la dirección IP

10.1.1.1. Cuando R3 intenta enviar un paquete de vuelta a 10.1.1.1, R3 tiene dos rutas que coinciden con la dirección de destino. Pero R3 toma la ruta más específica (prefijo más largo) para la subred 10.1.1.0/26. Esta ruta provoca que R3 reenvíe paquetes dirigidos a 10.1.1.1 por el enlace de R3 a R2, en lugar de a R1.

Aunque no necesariamente se determine el verdadero propósito de esta ruta estática, este proceso ha identificado la causa raíz: la ruta estática a 10.1.1.0/26 en R3. Si la LAN de R1 debe incluir todas las direcciones entre 10.1.1.0 y 10.1.1.255, la ruta estática podría ser borrada.

Un proceso de resolución de problemas alternativo para los Pasos 3, 4 y 5

Los pasos orientados a router del proceso de aislamiento de problemas de enrutamiento IP dependen del comando traceroute, confiando en la habilidad de este comando para identificar en qué router debe comenzar la resolución de problemas orientados a router. Los comandos ping y telnet se pueden utilizar como alternativa. Sin embargo, debido a que estos comandos no pueden identificar rápidamente los routers en los que es más probable que existan problemas, el uso de ping y telnet requiere que se realicen una serie de tareas en el primer router (el gateway / router predeterminado del host) en una ruta, y después en el siguiente router, y el siguiente, y así sucesivamente, hasta identificar el problema.

Por tanto, ya para terminar, observe que puede llevar a cabo las mismas subtareas específicas ya explicadas en los Pasos 4 y 5, pero utilizando ping, repita los pasos en cada router sucesivo. Por ejemplo, para aplicar este proceso revisado al primero de los dos escenarios que se acaban de completar, el proceso podría comenzar en el router R1, router predeterminado de PC1. En el primer escenario, R1 no tenía ningún problema en la ruta de reenvío de paquetes hacia 172.16.2.7 (PC4), y R1 no tenía problemas de ruta inversa ni de ACLs. Este nuevo proceso alternativo podría sugerir entonces pasar al siguiente router (R3). En este ejemplo, el problema de ruta de reenvío de R3 (no tener una ruta que coincida con la dirección de destino 172.16.2.7) se pondría de manifiesto.

Herramientas y pautas para la resolución de problemas

La segunda parte de este capítulo trata una amplia variedad de herramientas y pautas para la resolución de problemas que pueden ser útiles cuando se resuelven problemas en las redes reales. Alguna información de esta sección puede ser aplicada directamente a los exámenes CCNA. Otras partes de esta sección serán útiles indirectamente en los exámenes. La información puede ayudarle a aprender cómo trabajar con las redes en su trabajo, haciendo que esté mejor preparado no sólo para los escenarios únicos de los exámenes.

Perspectivas y herramientas de enrutamiento host

Esta sección trata dos temas cortos relativos a la forma en que los hosts procesan los paquetes IP. El primer tema muestra varias pautas para la resolución de problemas en los hosts. El segundo tema revisa la información tratada en el libro *CCENT/CCNA ICND1 Guía oficial para el examen de certificación* relativa a la forma en que la configuración de IP en un switch LAN funciona como un host.

Pautas para la resolución de problemas en los hosts

Cuando se trata de aislar la causa de los problemas de red, las pautas de la Tabla 7.4 pueden ayudar a encontrar más rápidamente los problemas relativos a los hosts. Las pautas están organizadas por los síntomas típicos, junto con la causa raíz más común. Observe que la tabla no muestra todas las posibles causas, sólo las más comunes.

Tabla 7.4. Síntomas más comunes de los problemas en los hosts y razones típicas.

Síntoma	**Causa raíz más común**
El host puede enviar paquetes a los hosts de la misma subred, pero no de otras subredes.	El host no tiene configurado un gateway predeterminado, o la dirección IP del gateway predeterminado es incorrecta.
El host puede enviar paquetes a los hosts de la misma subred, pero no de otras subredes.	El gateway predeterminado del host está en una subred diferente que la dirección IP del host (de acuerdo con la percepción que tiene el host de la subred).
Algunos hosts en una subred pueden comunicar con hosts de otras subredes, pero otros no.	Esto puede ser causado por un gateway (router) predeterminado utilizando una máscara diferente a la de los hosts. Esto puede resultar en que la ruta conectada del router no incluya algunos de los hosts de la LAN.
Algunos hosts en la misma VLAN pueden enviarse paquetes entre sí, pero otros no.	Los hosts pueden no estar utilizando la misma máscara.

Cuando se resuelven problemas de red en la vida real, es útil acostumbrarse a pensar en los síntomas, porque aquí es donde normalmente comienza el proceso de aislamiento del problema. Sin embargo, para los exámenes, la mayoría de los problemas de comunicación están provocados por un conjunto de problemas:

Paso 1 Verificar todos los hosts y routers que deben estar en la misma subred para asegurarse de que todos utilizan la misma máscara de subred y sus direcciones están de hecho en la misma subred.

Paso 2 Comparar la configuración de gateway predeterminado de cada host con la configuración del router para asegurarse de que es la dirección IP correcta.

Paso 3 Si los dos primeros datos son correctos, comprobar si hay problemas de capa 1/2, como se explicó en los Capítulos 1 a 3.

Soporte IP en switches LAN

Los switches Ethernet no necesitan conocer nada acerca de la capa 3 para realizar su función básica de capa 2 consistente en enviar tramas Ethernet. Sin embargo, para soportar varias características importantes, tales como la habilidad de hacer telnet y SSH al switch para resolver problemas, los switches LAN necesitan una dirección IP.

Los switches actúan como hosts cuando se configura IP. Comparado con un PC, un switch de Cisco no utiliza una NIC. En cambio, utiliza una interfaz virtual interna asociada con la VLAN 1 que esencialmente da al switch en sí mismo una interfaz en la VLAN 1. Entonces, la misma clase de elementos que se pueden configurar en un host para IP se pueden configurar en esta interfaz VLAN: dirección IP, máscara y gateway predeterminado. Las direcciones IP de los servidores DNS también se configuran.

La siguiente lista repite la lista de comprobación de la configuración IP de un switch ofrecida en el libro *CCENT/CCNA ICND1*. A continuación de la lista, el Ejemplo 7.6 muestra la dirección IP para el switch SW1 de la Figura 7.5.

Paso 1 Entrar en el modo de configuración de VLAN 1 usando el comando de configuración global `interface vlan 1` (desde cualquier modo de configuración).

Paso 2 Asignar una dirección IP y una máscara usando el subcomando de interfaz `ip address` *dirección-ip máscara*.

Paso 3 Habilitar la interfaz VLAN 1 usando el subcomando de interfaz `no shutdown`.

Paso 4 Añadir el subcomando global `ip default-gateway` *dirección-ip* para configurar el gateway predeterminado.

Ejemplo 7.6. Configuración de la dirección IP estática de un switch.

```
SW1#configure terminal
SW1(config)#interface vlan 1
SW1(config-if)#ip address 10.1.1.200 255.255.255.0
SW1(config-if)#no shutdown
00:25:07: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
00:25:08: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
  state to up
SW1(config-if)#exit
SW1(config)#ip default-gateway 10.1.1.1
```

NOTA

La interfaz VLAN en un switch está en un estado administrativamente desactivado hasta que el usuario ejecuta el comando no shutdown; el switch no puede enviar paquetes IP hasta que la interfaz VLAN 1 se activa.

Una precaución común cuando se configura o se resuelven problemas de conectividad IP en los switches LAN está relacionada con el *trunking* VLAN. Cisco generalmente sugiere que evite colocar dispositivos de usuario final en la VLAN 1; en cambio, la dirección IP del switch puede estar bien configurada en la VLAN 1. Para soportar la capacidad del switch de enviar y recibir paquetes a elementos situados en subredes diferentes, soportando por tanto Telnet en el switch desde estas subredes de usuario final, la configuración *trunking* del router debe incluir la configuración para la VLAN 1 así como las VLANs de usuario final.

Referencia de show ip route

El comando show ip route juega un papel importante en la resolución de problemas de enrutamiento IP y de los problemas de protocolo de enrutamiento IP. Muchos capítulos de este libro y del libro ICND1 mencionan varios factores acerca de este comando. Esta sección reúne los conceptos en un único lugar para una fácil referencia y estudio.

La Figura 7.6 muestra la salida del comando show ip route del anterior Ejemplo 7.3. La figura numera varias partes de la salida del comando para una más fácil referencia; la Tabla 7.5 describe la salida denotada con cada número.

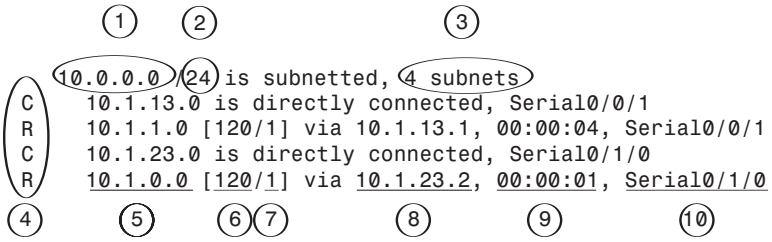


Figura 7.6. Referencia de la salida del comando **show ip route**.

La salida del comando difiere ligeramente cuando se utiliza VLSM. La figura muestra un ejemplo en el cual VLSM no se usa en la red 10.0.0.0, con máscara/24 utilizada para todas las subredes de esta red. Así, el IOS lista la máscara una vez, en la línea de encabezado (/24 en este caso). Si VLSM estuviera en uso, la línea de encabezado podría simplemente anotar que la red tiene subredes variables, y cada ruta podría listar la máscara. A modo de ejemplo, consulte el Ejemplo 5.1 del Capítulo 5, "VLSM y resumen de rutas".

Tabla 7.5 Descripción de la salida del comando **show ip route**.

N.º de elemento	Elemento	Valor en la Figura	Descripción
1	Red con clase	10.0.0.0	La tabla de enrutamiento está organizada por la red con clase. Esta línea es el encabezado para la red con clase 10.0.0.0.
2	Longitud de prefijo	/24	Cuando un router conoce sólo una máscara de subred para todas las subredes de la red, este lugar muestra esta única máscara, de forma predeterminada en notación con prefijo.
3	Número de subredes	4 subredes	Muestra el número de rutas para la subredes de la red con clase conocidas por este router.
4	Código de la leyenda	R, C	Un código corto que identifica el origen de la información de enrutamiento. R es para RIP, y C es para conectadas. La figura omite el texto de la leyenda en la parte superior de la salida del comando show ip route, pero se puede ver en el Ejemplo 7.3.
5	Número de subred	10.1.0.0	El número de subred de esta ruta en concreto.
6	Distancia administrativa (AD)	120	Si un router aprende rutas para la subred listada desde más de un origen de información de enrutamiento, el router utiliza el origen con menor AD.
7	Métrica	1	La métrica para esta ruta.
8	Router de siguiente salto	10.1.23.2	Para los paquetes coincidentes con esta ruta, la dirección IP del siguiente router por el cual el paquete debería ser reenviado.
9	Temporizador	00:00:01	Tiempo desde que esta ruta fue aprendida en una actualización de enrutamiento.
10	Interfaz de salida	Serial0/1/0	Para los paquetes coincidente con esta ruta, la interfaz de salida por la que el paquete debería ser reenviado.

Estado de la interfaz

Uno de los pasos del proceso de resolución de problemas de enrutamiento IP descrito anteriormente, en la sección "Resolución de problemas en el proceso de envío de paquetes", dice que se verifique el estado de la interfaz, asegurando que la interfaz requerida está funcionando. Para que una interfaz de router funcione, los dos códigos de estado de

la interfaz deben aparecer como "*up*"; los ingenieros suelen decir que la interfaz está "up y up" (*up and up*).

Este capítulo no explica los pasos de resolución de problemas para las interfaces de router, simplemente asume que cada interfaz está realmente en un estado *up*/*up*. La sección del Capítulo 12 titulada "Resolución de problemas en enlaces serie" trata muchos de los detalles de la resolución de problemas en interfaces de routers. Para las interfaces de router conectadas a un switch LAN, los elementos principales a verificar en los routers son que el router y el switch coincidan entre sí en las configuraciones de velocidad y del dúplex, y que si el *trunking* está configurado, tanto el router como el switch tienen que configurarse manualmente para el *trunking*, porque los routers no negocian dinámicamente el *trunking* LAN.

Problemas de VLSM

Esta sección examina varios problemas con el uso de VLSM:

- Reconocer si se está utilizando VLSM, y si es así, qué protocolo de enrutamiento puede ser utilizado.
- Entender las condiciones en las cuales los routers pueden permitir un error de configuración de subredes VLSM solapadas.
- Entender los síntomas externos que pueden ocurrir cuando existen subredes VLSM solapadas.

Forma de conocer cuándo se utiliza VLSM

Una equivocación común cuando se resuelve un problema en una internetwork desconocida es no reconocer si se está utilizando VLSM. Como se define en el Capítulo 5, una internetwork utiliza VLSM cuando se utilizan múltiples máscaras de subred para diferentes subredes de **una única red con clase**. Por ejemplo, si en una internetwork todas las subredes de la red 10.0.0.0 utilizan una máscara 255.255.240.0, y todas las subredes en la red 172.16.0.0 utilizan una máscara 255.255.255.0, el diseño no usa VLSM. Si se utilizaran múltiples máscaras en las subredes de la red 10.0.0.0, VLSM podría estar en uso.

El concepto siguiente es que sólo los protocolos de enrutamiento sin clase (RIP-2, EIGRP, OSPF) pueden soportar VLSM; los protocolos de enrutamiento con clase (RIP-1, IGRP) no pueden. Por tanto, una determinación rápida de si VLSM está actualmente usándose puede entonces decirle si se necesita un protocolo de enrutamiento sin clase. Observe que el protocolo de enrutamiento no necesita ninguna configuración especial para soportar VLSM. Es una característica del protocolo de enrutamiento.

Configuración de subredes VLSM solapadas

Las reglas del *subnetting* IP necesitan que los rangos de subredes utilizadas en una internetwork no se solapen. El IOS puede reconocer cuándo un nuevo comando ip address

crea una subred solapada, pero sólo en algunos casos. Esta sección examina las condiciones bajo las cuales se pueden configurar subredes solapadas, comenzando con las siguientes sentencias generales acerca de cuándo los solapamientos pueden o no ser configurados:

- **Previniendo el solapamiento:** el IOS detecta el solapamiento cuando el comando ip address implica un solapamiento con otro comando ip address **en el mismo router**. Si la interfaz que está siendo configurada está *up*/*up*, el IOS rechaza el comando ip address. Si no, el IOS acepta el comando ip address, pero nunca activará la interfaz.
- **Permitiendo el solapamiento:** el IOS no puede detectar un solapamiento cuando un comando ip address se solapa con un comando ip address en otro router.

El router mostrado en el Ejemplo 7.7 previene la configuración de una subred VLSM solapada. El ejemplo muestra al router R3 configurando Fa0/0 con la dirección IP 172.16.5.1/24, y Fa0/1 con 172.16.5.193/26. Los rangos de direcciones de cada subred son:

Subred 172.16.5.0/24: 172.16.5.1– 172.16.5.254
Subred 172.16.5.192/26: 172.16.5.193–172.16.5.254

Ejemplo 7.7. Subredes solapadas rechazadas en un único router.

```
R3#configure terminal
R3(config)#interface Fa0/0
R3(config-if)#ip address 172.16.5.1 255.255.255.0
R3(config-if)#interface Fa0/1
R3(config-if)#ip address 172.16.5.193 255.255.255.192
% 172.16.5.192 overlaps with FastEthernet0/0
R3(config-if)#
```

El IOS conoce que es ilegal solapar los rangos de direcciones implicados por una subred. En este caso, como ambas subredes pudieran ser subredes conectadas, este único router conoce que estas dos subredes no podrían coexistir, porque esto podría romper las reglas del *subnetting*; por tanto, el IOS rechaza el segundo comando.

Sin embargo, es posible configurar subredes solapadas si están conectadas a diferentes routers. La Figura 7.7 muestra una figura muy similar a la Figura 5.2 del Capítulo 5 (utilizado en este capítulo para explicar el problema de las subredes solapadas). El Ejemplo 7.8 muestra la configuración de las dos subredes solapadas en R2 y R3, con la tabla de enrutamiento resultante en R2.

Para los exámenes, tenga en mente que las subredes solapadas se pueden configurar si las subredes no conectan con el mismo router. Por tanto, si una pregunta pide elegir un nuevo número de subred y configurar una interfaz para pertenecer a esa subred, la aceptación del router del comando ip address no necesariamente indica que haya realizado los cálculos correctamente.

El siguiente tema explica los mismos síntomas del problema que usted puede observar si tal solapamiento existe.

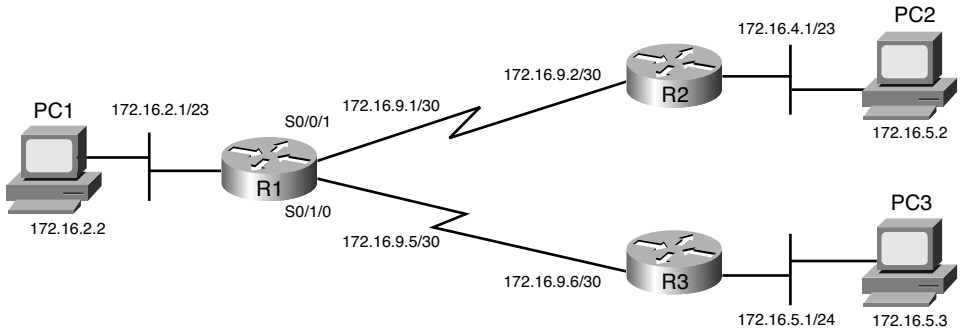


Figura 7.7. Internetwork que permite la configuración de subredes solapadas.

Ejemplo 7.8. Dos routers aceptan subredes solapadas.

```
SR2#configure terminal
R2(config)#interface Fa0/0
R2(config-if)#ip address 172.16.4.1 255.255.254.0
```

```
R3#configure terminal
R3(config)#interface Fa0/0
R3(config-if)# ip address 172.16.5.1 255.255.255.0
```

Síntomas de las subredes solapadas

NOTA

Aunque esta sección está incluida para completar este apartado, los tipos de problemas aquí descritos bien podrían estar fuera del alcance de los exámenes CCNA.

Los síntomas externos del problema difieren dependiendo de si la dirección en cuestión está en la porción solapada de la subred y si múltiples hosts intentan utilizar exactamente la misma dirección IP. Las direcciones en la parte no solapada de la subred normalmente funcionan bien, mientras que aquellas en el área solapada podrían funcionar o no. Por ejemplo, continuemos con las subredes solapadas mostradas en la Figura 7.6, las subredes solapadas 172.16.4.0/23 y 172.16.5.0/24 (concretamente, las direcciones 172.16.5.0–172.16.5.255). Los hosts que se hallen en el rango no solapado de 172.16.4.0–172.16.4.255 probablemente funcionarán bien.

Para las direcciones en el rango de direcciones solapadas, en muchos casos, los hosts de la menor de los dos subredes solapadas funcionan bien, pero los hosts de la mayor de las dos subredes no. Para ver por qué, considere el caso en el cual PC1 en la Figura 7.7 trata de hacer ping tanto a 172.16.5.2 (PC2, de R2) como a 172.16.5.3 (PC3, de R3). (A causa de este ejemplo, se asume que las direcciones de PC2 y PC3 no están duplicadas en la subred solapada opuesta.) Como puede ver en las tablas de enrutamiento de R1 y R3 y el comando

traceroute 172.16.5.2 del Ejemplo 7.9, el paquete enviado por PC1 a PC2 podría realmente ser entregado desde R1 a R3, y después en la LAN de R3.

Ejemplo 7.9. Dos routers aceptan subredes solapadas.

```
! La ruta de R1 para alcanzar 172.16.5.2, de R2, apunta a R3
R1#show ip route 172.16.5.2
Routing entry for 172.16.5.0/24
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 172.16.9.6 on Serial0/1/0, 00:00:25 ago
  Routing Descriptor Blocks:
  * 172.16.9.6, from 172.16.9.6, 00:00:25 ago, via Serial0/1/0
      Route metric is 1, traffic share count is 1
! La ruta de R1 para alcanzar 172.16.5.3, de R3, apunta a R3
R1#show ip route 172.16.5.3
Routing entry for 172.16.5.0/24
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 172.16.9.6 on Serial0/1/0, 00:00:01 ago
  Routing Descriptor Blocks:
  * 172.16.9.6, from 172.16.9.6, 00:00:01 ago, via Serial0/1/0
      Route metric is 1, traffic share count is 1

! El traceroute a PC2 muestra R3, no R2, como primer router, por lo que el paquete
! nunca alcanza PC2, y el comando no se detiene hasta que lo finaliza el usuario.
R1#traceroute 172.16.5.2

Type escape sequence to abort.
Tracing the route to 172.16.5.2

  1 172.16.9.6 4 msec 0 msec 4 msec
  2 * * *
  3 * * *
  4
R1#traceroute 172.16.5.3

Type escape sequence to abort.
Tracing the route to 172.16.5.3

  1 172.16.9.6 0 msec 4 msec 0 msec
  2 172.16.5.3 4 msec * 0 msec
```

El ejemplo muestra que R1 envía paquetes a los hosts 172.16.5.2 (PC2) y 172.16.5.3 (PC3) enviándolos a R3 a continuación. R3 entonces trata de enviarlos a la subred LAN de R3, que funciona bien para PC3 pero no tan bien para PC2. Así, PC3, en la menor de las dos subredes solapadas, funciona bien, mientras que PC2, en la mayor de las dos subredes solapadas, no lo hace.

Los síntomas pueden ser aún peores cuando las direcciones se duplican. Por ejemplo, imagine que se añade PC22 a la subred LAN de R2, con la dirección IP 172.16.5.3 duplicando la dirección IP de PC3. Ahora, cuando el usuario de PC22 llama para decir que su PC no comunica con otros dispositivos, el personal de soporte de red utiliza un ping 172.16.5.3 para verificar el problema, ¡y el ping funciona! El ping funciona para la instancia errónea de 172.16.5.3, pero funciona. Por tanto, los síntomas pueden ser particularmente difíciles de rastrear.

Otra dificultad con las subredes VLSM solapadas es que el problema puede no presentarse durante algún tiempo. En el mismo ejemplo, imagine que todas las direcciones en ambas subredes fueron asignadas por un servidor DHCP, comenzando con las direcciones IP menores. Durante los primeros seis meses, el servidor asignó sólo direcciones IP que comenzaban por 172.16.4.*x* en la subred LAN de R2. Finalmente, se instalaron suficientes hosts en la LAN de R2 como para que se necesitase el uso de direcciones que comienzan por 172.16.5, como la dirección de PC2, 172.16.5.2, utilizada en el ejemplo precedente.

Desafortunadamente, nadie puede enviar paquetes a estos hosts. A primera vista, el hecho de que el problema se muestre mucho tiempo después de que la instalación y la configuración se completaran puede realmente ocultar el problema.

Resumen de la resolución de problemas de VLSM

La siguiente lista resume los puntos clave de la resolución de problemas a considerar cuando se solucionan potenciales problemas de VLSM en los exámenes:

- Preste especial atención a si el diseño realmente utiliza VLSM. Si lo hace, observe si se está utilizando un protocolo de enrutamiento sin clase. Tema clave
- Sea consciente de que de hecho se pueden configurar subredes solapadas.
- Los síntomas exteriores del problema pueden ser que algunos hosts de una subred funcionan bien, pero otros no pueden enviar paquetes fuera de la subred local.
- Utilice el comando traceroute para buscar rutas que dirijan paquetes a la parte errónea de la red. Esto puede ser un resultado de las subredes solapadas.
- En los exámenes, se puede dar una pregunta que usted piense que es relativa a VLSM y a las direcciones IP. En este caso, el mejor plan de ataque puede ser bien analizar la matemática de cada subred y asegurarse de que no existe solapamiento, o bien resolver el problema utilizando ping y traceroute.

Redes discontinuas y autoresumen

El capítulo 5 explicó el concepto de redes discontinuas o separadas, junto con la solución: utilizar un protocolo de enrutamiento sin clase con autoresumen deshabilitado. Esta sección examina un caso particular en el cual una red discontinua existe sólo parte del tiempo. La Figura 7.8 muestra una internetwork con dos redes con clase: 10.0.0.0 y 172.16.0.0. El diseño muestra dos redes contiguas porque entre todas las subredes de la red existe una ruta compuesta únicamente de las subredes de cada red.

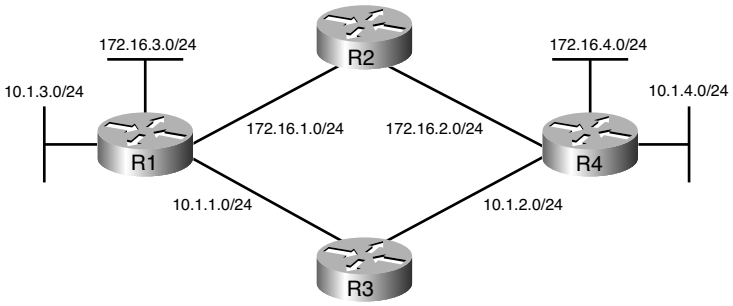


Figura 7.8. Internetwork con redes (actualmente) contiguas.

En esta figura con todos los enlaces activos y funcionando, utilizando un protocolo de unrutamiento con el autoresumen habilitado de forma predeterminada, todos los hosts pueden hacer ping a todos los otros hosts. En este diseño, los paquetes para la red 172.16.0.0 fluyen por la ruta superior, y los paquetes para la red 10.0.0.0 fluyen a través de la ruta inferior.

Desafortunadamente, un problema puede ocurrir más tarde cuando uno de los cuatro enlaces entre los routers falle. Si algún enlace entre los routers falla, una de las dos redes con clase llega a ser discontinua. Por ejemplo, si el enlace entre R3 y R4 falla, la ruta de R1 hacia R4 pasa a través de subredes de la red 172.16.0.0, por lo que la red 10.0.0.0 es discontinua. Incluso con un protocolo de enrutamiento sin clase, pero con el autoresumen habilitado, R1 y R4 publican una ruta para 10.0.0.0/8 hacia R2, y R2 ve dos rutas a todo lo de la red 10.0.0.0: una a través de R1, y otra a través de R4. La solución, como siempre, es el uso de un protocolo de enrutamiento sin clase con el autoresumen deshabilitado.

Aunque el diseño de la Figura 7.8 puede parecer un poco artificial, sucede más a menudo de lo que se puede pensar; concretamente cuando las compañías se compran y se venden. Tanto en la vida real como en los exámenes, tenga presente el concepto de redes discontinuas para casos operativos y para casos en los cuales fallan los enlaces redundantes.

Pautas para la resolución de problemas en las listas de acceso

La resolución de los problemas provocados por las ACLs pueden bien ser una de las áreas más difíciles en el trabajo con redes reales. Una de las mayores dificultades es que las herramientas tradicionales de resolución de problemas, tales como ping y traceroute, no envían paquetes que se parezcan a los paquetes coincidentes con la variedad de campos de las ACLs extendidas. Por tanto, aunque un ping puede funcionar, el hosts de usuario final puede no se capaz de alcanzar la aplicación correcta, o viceversa.

Esta sección resume algunos consejos para abordar los problemas relacionados con las ACLs en la vida real y en los exámenes:

Paso 1 Determinar en qué interfaces están habilitadas las ACLs, y en qué dirección (show running-config, show ip interfaces).

Paso 2 Determinar qué sentencias ACL coinciden con los paquetes de prueba (show access-lists, show ip access-lists).

Paso 3 Analizar las ACLs para predecir qué paquetes pueden coincidir con la ACL, centrándose en los siguientes puntos:

- **a.** Recordar que la ACL utiliza la lógica de primera coincidencia.
- **b.** Considerar el uso de la matemática (posiblemente) más rápida descrita en el Capítulo 6, "Listas de control de acceso IP", que convierte pares "dirección/máscara" de ACL en pares "dirección/máscara de subred" que permiten el uso de la misma matemática que las subredes.
- **c.** Observe la dirección del paquete en relación al servidor (hacia el servidor, desde el servidor). Asegurarse de que los paquetes tienen unos valores concretos de dirección IP de origen y puerto, o dirección IP de destino y puerto, cuando se procesan por la ACL habilitada para una dirección concreta (entrado o salida).
- **d.** Recordar que las palabras clave tcp y udp se deben utilizar si el comando necesita verificar los números de puerto. (Ver en la Tabla 6.5 del Capítulo 6 una lista de los números de puerto de TCP y UDP más populares.)
- **e.** Observe que los paquetes ICMP no utilizan UDP o TCP. ICMP es considerado otro protocolo que coincide con la palabra clave icmp (en vez de ip, tcp y udp).
- **f.** En lugar de usar la denegación implícita al final de cada ACL, utilizar el comando de configuración explícito para denegar todo el tráfico al final de la ACL para que los contadores del comando show se incrementen cuando se tome esa acción.

El capítulo 6 trata la información subyacente a los consejos del Paso 3. El recordatorio de esta sección se centra en los comandos disponibles para investigar los problemas en los dos primeros pasos.

Si hay un problema en el envío de paquetes IP, y las ACLs existentes pueden influir en el problema, el primer paso para aislar el problema es encontrar la ubicación y dirección de las ACLs. La forma más rápida de hacer esto es buscar en la salida del comando show running-config y buscar en los comandos ip access-group en cada interfaz. Sin embargo, en muchos casos, puede no estar permitido el acceso al modo de activación, y se necesitan los comandos show. La única forma de encontrar las interfaces y la dirección de las ACLs IP es el comando show ip interfaces, como muestra el Ejemplo 7.10.

Observe que la salida del comando lista si una ACL está habilitada, en ambas direcciones, y qué ACL es. El ejemplo muestra una versión abreviada del comando show ip interface S0/0/1, que lista los mensajes para esta interfaz. El comando show ip interface podría listar los mismos mensajes para toda interfaz del router.

Ejemplo 7.10. Ejemplo del comando **show ip interface**.

```
R1>show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet address is 10.1.2.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.9
  Outgoing access list is not set
  Inbound access list is 102
! Para abreviar se han omitido aproximadamente 26 líneas
```

El Paso 2 dice que se encuentre el contenido de la ACL. De nuevo, la forma más rápida de ver la ACL es utilizar el comando show running-config. Si el modo de activación está permitido, los comando show access-lists y show ip access-lists proporcionan la misma salida. La única diferencia es que si se han configurado otras ACLs no IP, el comando show access-lists lista también las ACLs no IP. La salida proporciona los mismos detalles mostrados en los comandos de configuración, así como un contador para el número de paquetes coincidentes con cada línea de la ACL. El Ejemplo 7.11 muestra un ejemplo.

Ejemplo 7.11. Ejemplo del comando **show ip access-lists**.

```
R1#show ip access-lists
Extended IP access list 102
    10 permit ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255 (15 matches)
```

Después de las ubicaciones, las direcciones y los detalles de configuración de las ACLs descubiertos en los Pasos 1 y 2, comienza la parte dura: interpretar qué hace realmente la ACL. De interés particular es el último elemento en la lista de las pautas de resolución de problemas, elemento 3E. En la ACL mostrada en el Ejemplo 7.11, algunos paquetes (15 hasta ahora) han coincidido con la única sentencia access-list configurada en la ACL 102. Sin embargo, algunos paquetes han sido probablemente denegados por la aplicación de la lógica implícita de denegar todos los paquetes al final de una ACL. Si se utiliza en la configuración el comando access-list 102 deny ip any any al final de la ACL, que explícitamente coincide con todos los paquetes y los descarta, el comando show ip access-lists podría entonces mostrar el número de paquetes denegados al final de la ACL. Cisco recomienda a veces añadir explícitamente la sentencia de denegar al final de la ACL para una más fácil resolución de los problemas.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 7.6 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 7.6. Temas clave del Capítulo 7.

Tema clave	Descripción	Número de página
Tabla 7.1	Mensajes ICMP comunes y su propósito.	267
Figura 7.3	Diagrama de cómo funcionan el campo TTL de la cabecera IP y el mensaje de tiempo excedido.	272
Figura 7.4	Demostración de cómo el comando traceroute utiliza el campo TTL y el mensaje de tiempo excedido.	273
Lista	Los dos pasos principales y varios subpasos del proceso sugerido de aislamiento de un problema de enrutamiento en el host.	275-276
Lista	Los tres pasos principales del aislamiento de un problema con el enrutamiento IP en los routers; la lista se ofrece numerada como continuación de la lista de aislamiento de un problema de enrutamiento.	277-278
Lista	Tres consejos a tener en cuenta a la hora de resolver problemas de conectividad de un host.	286
Lista	Lista de los pasos de configuración de los detalles IP de un switch LAN.	286
Lista	Condiciones bajo las que se puede configurar el solapamiento de subredes, y cuándo el IOS puede evitar este error.	290
Lista	Resumen de los consejos de resolución de problemas para las preguntas en las que VLSM puede provocar un problema.	293
Lista	Tres pasos para resolver problemas con las ACLs, particularmente cuando no se puede visualizar la configuración.	295

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD) o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe sus respuestas en el glosario:

Ruta de envío, ruta inversa.

Temas del examen* ICND2 publicados por Cisco que se tratan en esta parte

Implementación de un esquema de direccionamiento IP y de servicios IP para cumplir los requisitos de red de la red de la sede de una empresa de tamaño medio

- Identificar y corregir problemas comunes asociados con el direccionamiento IP y las configuraciones de los hosts.

Configuración y resolución de problemas para el funcionamiento básico y el enrutamiento de dispositivos Cisco

- Comparar y contrastar métodos de enrutamiento y protocolos de enrutamiento.
- Configurar, verificar y resolver problemas de OSPF.
- Configurar, verificar y resolver problemas de EIGRP.
- Verificar la configuración y la conectividad utilizando ping, traceroute y telnet o SSH.
- Resolver problemas de implementación de enrutamiento.
- Verificar el funcionamiento del hardware y del software empleando comandos SHOW y DEBUG.

* No olvide consultar en http://www.cisco.com los últimos temas de examen publicados.

PARTE III

Configuración y resolución de problemas con los protocolos de enrutamiento

Capítulo 8 Teoría de los protocolos de enrutamiento

Capítulo 9 OSPF

Capítulo 10 EIGRP

Capítulo 11 Resolución de problemas en los protocolos de enrutamiento

Este capítulo trata los siguientes temas:

Descripción del protocolo de enrutamiento dinámico: Esta sección introduce los conceptos base que hay detrás de cómo funcionan los protocolos de enrutamiento y muchos términos relativos a los protocolos de enrutamiento.

Características del protocolo de enrutamiento por vector de distancia: Esta sección explica cómo funcionan los protocolos por vector de distancia, centrándose en las características que permiten evitar los bucles.

Características del protocolo de enrutamiento por estado del enlace: Esta sección explica cómo funcionan los protocolos de enrutamiento por estado del enlace, utilizando OSPF como un ejemplo concreto.

CAPÍTULO 8

Teoría de los protocolos de enrutamiento

La Parte II, "Enrutamiento IP", se centra en el proceso de enrutamiento IP (envío de paquetes), tratando también el tema de cómo los routers rellenan sus tablas de enrutamiento. La Parte III, "Configuración y resolución de problemas con los protocolos de enrutamiento", que comienza con este capítulo, centra el interés en cómo los routers rellenan sus tablas de enrutamiento utilizando los protocolos de enrutamiento dinámico.

Los protocolos de enrutamiento IP funcionan en un conjunto de routers, enviando mensajes a sus routers vecinos para ayudar a estos routers a aprender todas las mejores rutas a cada subred. Aunque este objetivo es simple, los procesos utilizados por los protocolos de enrutamiento tienden a ser algo más complejos y a ser temas importantes en los exámenes de CCNA. Este capítulo comienza el tratamiento de los protocolos de enrutamiento IP explicando los conceptos y la teoría fundamentales que están detrás de su funcionamiento. Los Capítulos 9 y 10 van a proporcionar mucho más detalle acerca de cómo funcionan OSPF y EIGRP, respectivamente. El Capítulo 11 finaliza esta parte del libro examinando algunos procesos de resolución de problemas y pautas para OSPF y EIGRP.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las diez preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 8.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

Tabla 8.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
Descripción del protocolo de enrutamiento dinámico	1-5
Características del protocolo de enrutamiento por vector de distancia	6-8
Características del protocolo de enrutamiento por estado del enlace	9 y 10

1. ¿Cuáles de los siguientes protocolos utilizan la lógica por vector de distancia?
   - **a.** RIP-1
   - **b.** RIP-2
   - **c.** EIGRP
   - **d.** OSPF
   - **e.** BGP
   - **f.** IS-IS Integrado
2. ¿Cuáles de los siguientes protocolos utilizan la lógica por estado del enlace?
   - **a.** RIP-1
   - **b.** RIP-2
   - **c.** EIGRP
   - **d.** OSPF
   - **e.** BGP
   - **f.** IS-IS Integrado
3. ¿Cuál de los siguientes protocolos de enrutamiento utiliza una métrica que está, de forma predeterminada, al menos parcialmente afectada por el ancho de banda del enlace?
   - **a.** RIP-1
   - **b.** RIP-2
   - **c.** EIGRP
   - **d.** OSPF
   - **e.** BGP
4. ¿Cuál de los siguientes protocolos de enrutamiento interior soporta VLSM?
   - **a.** RIP-1
   - **b.** RIP-2
   - **c.** EIGRP
   - **d.** OSPF
   - **e.** IS-IS Integrado

5. ¿Cuál de las siguientes situaciones podría causar en un router que utiliza RIP-2 la eliminación de todas las rutas aprendidas desde un router vecino en particular?

a. Un fallo de actividad de RIP.

b. No recibir más actualizaciones de ese vecino.

c. Actualizaciones recibidas 5 o más segundos después de que la última actualización fuera enviada por este vecino.

d. Actualizaciones de este vecino con el indicador global "ruta mala".

6. ¿Cuál de las siguientes características del vector de distancia previene bucles de enrutamiento haciendo que el protocolo de enrutamiento publique sólo un subconjunto de rutas conocidas, en comparación con la tabla completa de enrutamiento, bajo unas condiciones normales estables?

a. Recuento hasta infinito.

b. Inversa envenenada.

c. *Holddown*.

d. Horizonte dividido.

e. Envenenamiento de ruta.

7. ¿Cuál de las siguientes características del vector de distancias previene bucles de enrutamiento publicando una ruta de métrica infinita cuando falla una ruta?

a. *Holddown*.

b. Actualizaciones completas.

c. Horizonte dividido.

d. Envenenamiento de ruta.

8. Un router que está utilizando un protocolo por vector de distancia acaba de recibir una actualización de enrutamiento que lista una ruta con una métrica infinita. La actualización de enrutamiento previa de este vecino listaba una métrica válida. ¿Cuál de lo siguiente no es una reacción normal a este escenario?

a. Enviar inmediatamente una actualización parcial que incluya una ruta envenenada para la ruta que falla.

b. Colocar la ruta en un estado *Holddown*.

c. Suspender el horizonte dividido para esta ruta y enviar una ruta inversa envenenada.

d. Enviar una actualización completa especificando una ruta envenenada para la ruta que falla.

9. Una internetwork está utilizando un protocolo de enrutamiento por estado del enlace. Los routers han inundado todas las LSAs, y la red está estable. ¿Cuál de lo siguiente describe por qué los routers han reinundado las LSAs?

a. Cada router reinunda cada LSA utilizando un tiempo periódico que es un tiempo similar a los temporizadores de actualización del vector de distancia.

b. Cada router reinunda cada LSA utilizando un temporizador periódico que es más largo que los temporizadores de actualizaciones por vector de distancia.

c. Los routers nunca reinundan las LSAs con tal de que las LSAs no cambien.

d. Los routers reinundan todas las LSAs siempre que una LSA cambia.

10. ¿Cuál de lo siguiente es verdad acerca de cómo un router utilizando un protocolo de enrutamiento por estado del enlace elige la mejor ruta a cada subred?

a. El router encuentra la mejor ruta en la base de datos de estado del enlace.

b. El router calcula la mejor ruta ejecutando el algoritmo SPF contra la información de la base de datos de estado del enlace.

c. El router compara la métrica listada para esa subred en las actualizaciones recibidas de cada vecino y elige la ruta de métrica mejor (más corta).

Temas fundamentales

Los protocolos de enrutamiento definen varias formas en que los routers dialogan entre ellos para determinar las mejores rutas a cada destino. Así como las redes con el paso del tiempo crecieron en complejidad, los routers ganaron en potencia y RAM. Como resultado, los ingenieros diseñaron nuevos protocolos de enrutamiento, tomando las ventajas de los enlaces y routers más rápidos, transformando los protocolos de enrutamiento. Este capítulo sigue hasta cierto punto esta progresión, comenzando con una introducción a los protocolos de enrutamiento. A continuación, se explica la teoría que está detrás de los protocolos de enrutamiento por vector de distancia, utilizada en los primeros protocolos de enrutamiento IP. La sección final de este capítulo examina la teoría de los protocolos de enrutamiento por estado del enlace, que se utiliza en algunos de los protocolos de enrutamiento más recientemente definidos.

Descripción del protocolo de enrutamiento dinámico

Nota

Si está utilizando el plan de lectura sugerido en la Introducción, ya debería haber leído acerca de los protocolos de enrutamiento en *CCENT/CCNA ICND1 Guía oficial para el examen de certificación*. Si es así, puede avanzar en este texto hasta la sección "Comparaciones de IGP: resumen", ya que muchas de las siguientes páginas tratan temas ya abordados en el Capítulo 14 del libro ICND1.

Los routers añaden rutas IP a sus tablas de enrutamiento utilizando tres métodos: rutas conectadas, rutas estáticas y rutas aprendidas utilizando los protocolos de enruta-

miento dinámico. Antes de ir más lejos en la discusión es importante definir unos pocos términos relacionados para aclarar cualquier concepto erróneo acerca de los términos **protocolo de enrutamiento, protocolo enrutado**, y **protocolo enrutable**. Los conceptos alrededor de estos términos no son difíciles, pero como son tan similares, y debido a que muchos documentos prestan poca atención a dónde utilizar cada uno de los términos, pueden ser un poco confusos. Estos términos generalmente se definen como sigue:

- **Protocolo de enrutamiento:** Un conjunto de mensajes, reglas y algoritmos utilizados por los routers para todos los propósitos de aprendizaje de rutas. Este proceso incluye cambio y análisis de la información de enrutamiento. Cada router elige la mejor ruta a cada subred (selección de ruta) y finalmente coloca estas mejores rutas en su tabla de enrutamiento IP. RIP, EIGRP, OSPF y BGP son algunos ejemplos.
- **Protocolo enrutado** y **protocolo enrutable:** Ambos términos se refieren a un protocolo que define la estructura de un paquete y el direccionamiento lógico, permitiendo a los routers enviar o enrutar los paquetes. Los routers envían, o enrutan, paquetes definidos por los protocolos enrutados o enrutables. Los ejemplos incluyen IP e IPX (una parte del modelo de protocolo de Novell NetWare).

Nota

El término **selección de ruta** a veces se refiere a parte del trabajo de un protocolo de enrutamiento, en el cual el protocolo de enrutamiento elige la mejor ruta.

Aunque los protocolos de enrutamiento (tal como RIP) son diferentes a los protocolos enrutados (tal como IP), trabajan muy estrechamente. El proceso de enrutamiento envía paquetes IP, pero si un router no tiene ninguna ruta en su tabla de enrutamiento que coincida con la dirección de destino del paquete, el router descarta el paquete. Los routers necesitan los protocolos de enrutamiento con los que aprender todas las posibles rutas y añadirlas a su tabla de enrutamiento para que el proceso de enrutamiento pueda enviar (enrutar) protocolos enrutables tales como IP.

Funciones del protocolo de enrutamiento

El software IOS de Cisco soporta varios protocolos de enrutamiento IP, que realizan las mismas funciones generales:

1. Aprender la información de enrutamiento acerca de las subredes IP de otros routers vecinos.
2. Publicar información de enrutamiento acerca de las subredes IP a otros routers vecinos.
3. Si existe más de una ruta posible para alcanzar una subred, elegir la mejor ruta basándose en una métrica.

4. Si la topología de la red cambia (por ejemplo, falla un enlace) reaccionar publicando que algunas rutas han fallado, y seleccionar una nueva ruta actualmente mejor. (Este proceso se denomina convergencia.)

Nota

Cuando un router se conecta al mismo enlace (por ejemplo, el mismo enlace WAN o la misma LAN Ethernet) que otro, se dice que los dos routers son vecinos.

La Figura 8.1 muestra un ejemplo de tres de las cuatro funciones de la lista. R1 y R3 aprenden una ruta a la subred 172.16.3.0/24 desde R2 (función 1). Después, R3 aprende la ruta a 172.16.3.0/24 desde R2; R3 publica esta ruta a R1 (función 2). Entonces R1 debe tomar una decisión acerca de las dos rutas aprendidas para alcanzar la subred 172.16.3.0/24: una con métrica 1 desde R2, y otra con métrica 2 desde R3. R1 elige la ruta de métrica menor a través de R2 (función 3).

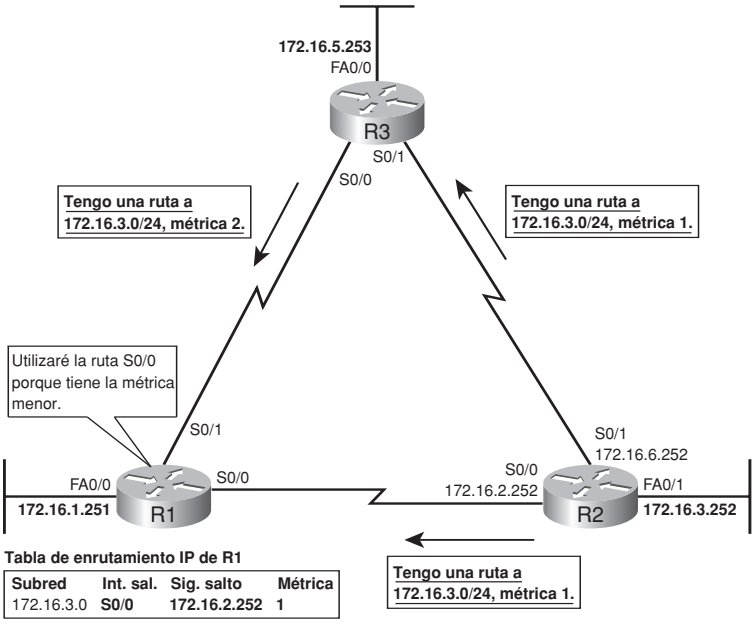


Figura 8.1. Tres de las cuatro funciones de los protocolos de enrutamiento.

La convergencia es la cuarta función de un protocolo de enrutamiento listada aquí. El término **convergencia** se refiere a un proceso que ocurre cuando cambian las topologías; esto es, cuando un enlace o un router falla o vuelven a estar activos de nuevo. Cuando algo cambia, las mejores rutas disponibles en la red pueden cambiar. La convergencia simplemente se refiere al proceso por el cual todos los routers comprenden colectivamente que algo ha cambiado, publican la información acerca de los cambios a todos los otros routers

y entonces eligen las rutas actualmente mejores para cada subred. La habilidad de converger rápidamente, sin causar bucles, es una de las consideraciones más importantes cuando se selecciona qué protocolo de enrutamiento IP utilizar.

En la Figura 8.1 la convergencia puede tener lugar si el enlace entre R1 y R2 falla. En este caso, R1 debe dejar de usar la vieja ruta para la subred 172.16.3.0/24 (directamente por R2), enviando en cambio paquetes a R3.

Los protocolos de enrutamiento exteriores e interiores

Los protocolos de enrutamiento IP se clasifican en dos categorías principales: **Protocolos de gateway interior** *(IGP, Interior Gateway Protocols)* o **Protocolos de gateway exterior** *(EGP, Exterior Gateway Protocols)*. Las definiciones de cada uno son las siguientes:

- **IGP:** Un protocolo de enrutamiento que fue diseñado y pensado para el uso en un único sistema autónomo (AS).
- **EGP:** Un protocolo de enrutamiento que fue diseñado y pensado para el uso entre diferentes sistemas autónomos.

Nota

Los términos IGP y EGP incluyen la palabra gateway porque los routers se denominaban gateways (pasarelas).

Estas definiciones utilizan un nuevo término: sistema autónomo (AS). Un AS es una internetwork bajo el control administrativo de una única organización. Por ejemplo, una internetwork creada y pagada por una única compañía es probablemente un único AS, y una internetwork creada por un único sistema escolar es probablemente un único AS. Otros ejemplos incluyen grandes divisiones de un estado o gobierno nacional, donde diferentes agencias gubernamentales pueden construir sus propias internetworks. Cada ISP es también normalmente un único AS diferente.

Algunos protocolos de enrutamiento funcionan mejor dentro de un único AS por diseño; por tanto, estos protocolos de enrutamiento se denominan IGPs. Coloquialmente, los protocolos de enrutamiento designados para intercambiar rutas entre routers de sistemas autónomos diferentes se denominan EGPs. (Actualmente, sólo existe un EGP legítimo: el Protocolo de gateway fronterizo [BGP, *Border Gateway Protocol*].)

Cada AS debe tener asignado un número llamado (sin sorpresa) **número AS (ASN)**. Igual que las direcciones IP públicas, la Corporación de Internet para la asignación de números de red (ICANN, http://www.icann.org) controla los derechos mundiales para asignar los ASNs. Este organismo delega su autoridad en otras organizaciones de todo el mundo, típicamente las mismas organizaciones que asignan direcciones IP públicas. Por ejemplo, en Norte América, el Registro americano para el registro de números de Internet (ARIN, http://www.arin.net/) asigna las direcciones IP públicas y los ASNs.

La Figura 8.2 muestra una pequeña vista de la Internet mundial. La figura muestra dos empresas y tres ISPs usando IGPs (OSPF y EIGRP) dentro de sus propias redes, y BGP entre los ASNs.

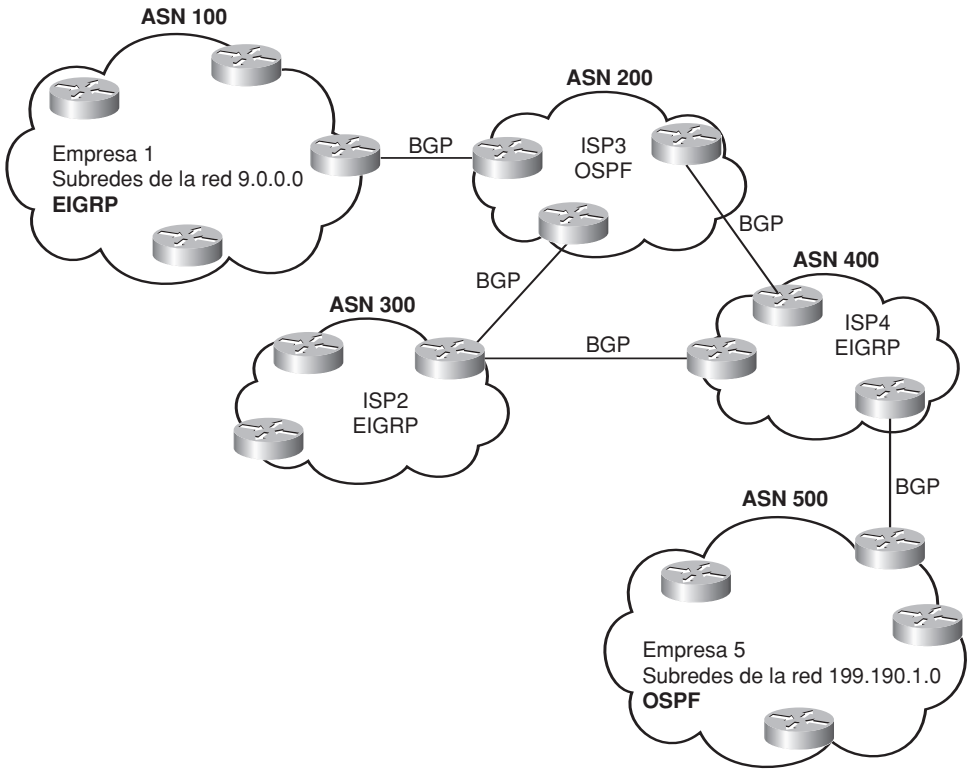


Figura 8.2. Comparando dónde utilizar IGPs y EGPs.

Comparando IGPs

Hoy en día, no hay una elección real sobre qué EGP utilizar: simplemente se utiliza BGP. Sin embargo, cuando se elige utilizar un IGP dentro de una única organización, existen varias opciones. Hoy las opciones más razonables son RIP-2, EIGRP y OSPF. Uno de estos tres IGPs, RIP-2, ya ha sido tratado con alguna profundidad en el libro **CCENT/CCNA ICND1**, y este libro trata OSPF y EIGRP con más profundidad en los Capítulos 9 y 10, respectivamente. Esta sección introduce algunos puntos claves de la comparación entre los IGPs IP.

Algoritmos de los protocolos de enrutamiento IGP

Un algoritmo subyacente a un protocolo de enrutamiento determina cómo dicho protocolo hace su trabajo. El término **algoritmo de protocolo de enrutamiento** simplemente

se refiere a la lógica y los procesos utilizados por los diferentes protocolos de enrutamiento para resolver los problemas de aprendizaje de todas las rutas, eligiendo la mejor ruta para cada subred, y convergiendo en reacción a los cambios en la internetwork. Existen tres ramas principales de los algoritmos de protocolo de enrutamiento para los protocolos de enrutamiento IGP:

- Vector de distancia (algunas veces llamado de Bellman-Ford por su creador).
- Estado del enlace.
- Híbrido equilibrado (a veces denominado vector de distancia mejorado).

Históricamente hablando, los protocolos por vector de distancia fueron inventados primero, principalmente en los primeros años de los 80. RIP fue el primer protocolo por vector de distancia IP utilizado, siendo el Protocolo de enrutamiento de gateway interior propietario de Cisco (IGRP, *Interior Gateway Routing Protocol*) introducido un poco más tarde. Pero en los 90, la convergencia un tanto lenta y la potencial creación de bucles de los protocolos por vector de distancia condujeron al desarrollo de nuevos protocolos de enrutamiento alternativos que utilizaran nuevos algoritmos. Los protocolos por estado del enlace (en concreto, OSPF e IS-IS Integrado) solucionaron los principales problemas de los protocolos por vector de distancia, pero necesitan de una mayor planificación en redes de tamaño medio y grande.

Aproximadamente al mismo tiempo que la introducción de OSPF, Cisco crea un protocolo de enrutamiento propietario llamado Protocolo de enrutamiento de gateway interior mejorado (EIGRP, *Enhanced Interior Gateway Routing Protocol*), que utiliza algunas de las características del anterior protocolo, IGRP. EIGRP soluciona los mismos problemas que los protocolos de enrutamiento por estado del enlace, pero se necesitaba menos planificación para su implementación en una red. Con el paso del tiempo, EIGRP fue clasificado como el único tipo de protocolo de enrutamiento (ni vector de distancia ni estado del enlace) por lo que EIGRP fue llamado bien un protocolo híbrido equilibrado o bien un protocolo por vector de distancia mejorado.

La segunda y tercera secciones de este capítulo examinan los algoritmos por vector de distancia y de estado del enlace en más detalle. El Capítulo 10 explica los conceptos de híbrido equilibrado en el contexto de la discusión de EIGRP.

Métricas

Los protocolos de enrutamiento eligen la mejor ruta para alcanzar una subred eligiendo la ruta de métrica menor. Por ejemplo, RIP utiliza un contador del número de routers (saltos) entre un router y la subred de destino. La Tabla 8.2 lista los más importantes protocolos de enrutamiento IP para los exámenes de CCNA y algunos detalles de la métrica en cada caso.

Al contrario que RIP-1 y RIP-2, las métricas de OSPF y EIGRP dependen de los valores de ancho de banda de la interfaz. La Figura 8.3 compara el impacto de las métricas utilizadas por RIP y EIGRP.

Como se muestra en la parte superior de la figura, la ruta RIP del Router B para 10.1.1.0 apunta al Router A porque esta ruta tiene menor contador de salto (1) que la ruta a través

Tabla 8.2. Métricas IGP IP.

IGP	Métrica	Descripción
RIP-1, RIP-2	Contador de salto	El número de routers (saltos) entre un router y la subred de destino.
OSPF	Coste	La suma de todos los valores de coste de la interfaz para todos los enlaces en una ruta, con el coste predeterminado basándose en el ancho de banda de la interfaz.
EIGRP	Composición de ancho de banda y retardo	Calculado basándose en el enlace más lento de la ruta y el retardo acumulado asociado con cada interfaz en la ruta.

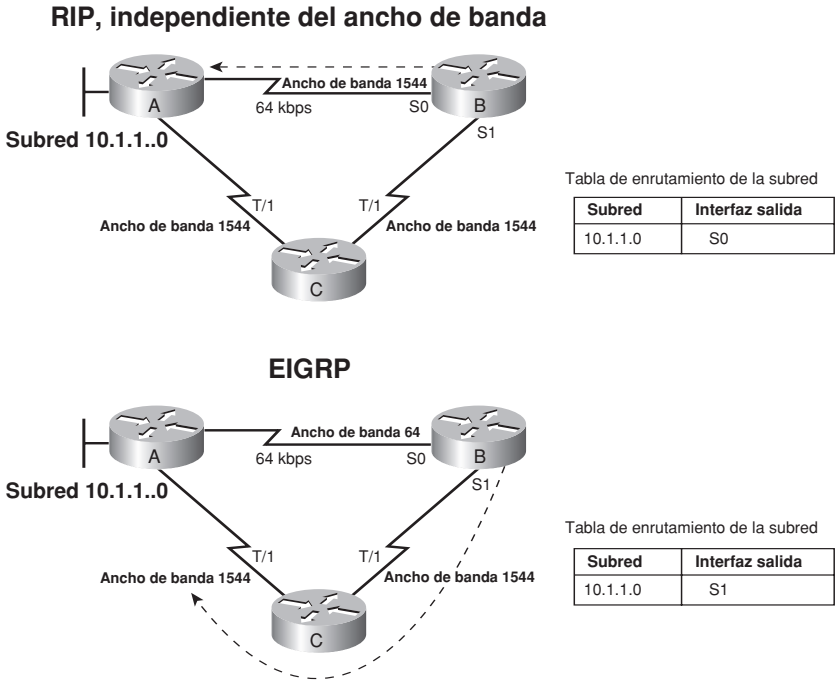


Figura 8.3. Métricas comparadas de RIP y EIGRP.

del Router C (2). Sin embargo, en la mitad inferior de la figura, el Router B elige la ruta de dos saltos a través del Router C cuando se utiliza EIGRP porque los anchos de banda de los dos enlace en la ruta son mucho más rápidos (mejores) que los de la ruta a un solo salto. Observe que para que EIGRP pueda realizar la elección correcta, el ingeniero configuró correctamente el ancho de banda de la interfaz para coincidir con la velocidad actual de los

enlaces; esto permite a EIGRP elegir la ruta mas rápida. (El subcomando de interfaz bandwidth no cambia la velocidad física actual de la interfaz. Sólo le dice al IOS qué velocidad asumir que está utilizando la interfaz.)

Comparaciones de IGP: resumen

Para una comparación conveniente y su estudio, la Tabla 8.3 resume muchas de las características soportadas por varios IGPs. La tabla incluye los elementos mencionados específicamente en este capítulo o en capítulos anteriores de este libro.

Tabla 8.3 Comparación de los protocolos de enrutamiento interior IP.

Característica	RIP-1	RIP-2	EIGRP	OSPF	IS-IS
Sin clase	No	Sí	Sí	Sí	Sí
Soporta VLSM	No	Sí	Sí	Sí	Sí
Envía máscara en la actualización	No	Sí	Sí	Sí	Sí
Vector de distancia	Sí	Sí	No[1]	No	No
Estado del enlace	No	No	No[1]	Sí	Sí
Soporta el autoresumen	No	Sí	Sí	No	No
Soporta el resumen manual	No	Sí	Sí	Sí	Sí
Propietario	No	No	Sí	No	No
Las actualizaciones de enrutamiento se envían a una dirección IP de multidifusión	No	Sí	Sí	Sí	—
Soporta la autenticación	No	Sí	Sí	Sí	Sí
Convergencia	Lenta	Lenta	Muy rápida	Rápida	Rápida

[1] EIGRP es descrito a menudo como un protocolo de enrutamiento híbrido equilibrado, en lugar de como estado del enlace o vector de distancia. Algunos documentos se refieren a EIGRP como un protocolo por vector de distancia avanzado.

Además de la Tabla 8.3, la Tabla 8.4 lista algunos otros temas acerca de RIP-2, OSPF y EIGRP. Los elementos de la Tabla 8.4 se explican de manera más amplia en los Capítulos 9 y 10, pero se incluyen aquí como referencia para su estudio.

Distancia administrativa

Muchas compañías y organizaciones utilizan un único protocolo de enrutamiento. Sin embargo, en algunos casos, una compañía necesita varios protocolos de enrutamiento. Por

Tema clave **Tabla 8.4.** Comparación de las características de los IGPs: RIP-2, EIGRP y OSPF.

Característica	RIP-2	OSPF	EIGRP
Métrica	Contador de salto	Coste del enlace	Función del ancho de banda, retardo
Envía actualizaciones periódicas	Sí (30 segundos)	No	No
Actualizaciones de enrutamiento completas o parciales	Completa	Parcial	Parcial
Dónde se envían las actualizaciones	(224.0.0.9)[1]	(224.0.0.5, 224.0.0.6)	(224.0.0.10)
Métrica considerada "infinita"	16	$(2^{24} - 1)$	$(2^{32} - 1)$
Soporta equilibrado de carga de coste no igual	No	No	Sí

[1] Esta tabla se refiere específicamente a las características de RIP-2, pero la única diferencia con RIP-1 en esta tabla es que RIP-1 difunde las actualizaciones a la dirección IP 255.255.255.255.

ejemplo, si dos compañías conectan sus redes para que puedan intercambiar información, necesitan intercambiar alguna información de enrutamiento. Si una compañía utiliza RIP, y la otra utiliza EIGRP, en al menos un router se deben utilizar RIP y EIGRP. Entonces, ese router puede obtener rutas aprendidas por RIP y publicarlas en EIGRP, y viceversa, a través de un proceso llamado redistribución de ruta.

Dependiendo de la topología de la red, los dos protocolos de enrutamiento podrían aprender rutas a las mismas subredes. Cuando un único protocolo de enrutamiento aprende múltiples rutas a la misma subred, la métrica le dice cuál es la mejor ruta. Sin embargo, cuando dos protocolos de enrutamiento diferentes aprenden rutas a la misma subred, como la métrica de cada protocolo de enrutamiento está basada en diferente información, el IOS no puede comparar las métricas. Por ejemplo, RIP podría aprender una ruta a la subred 10.1.1.0 con métrica 1, y EIGRP podría aprender una ruta a 10.1.1.0 con métrica 2.195.416, pero la de EIGRP podría ser la ruta mejor (o puede que no). Simplemente no hay una base para comparar entre las dos métricas.

Cuando el IOS debe elegir entre las rutas aprendidas utilizando diferentes protocolos de enrutamiento, el IOS utiliza un concepto llamado **distancia administrativa**. La distancia administrativa es un número que denota cómo es de creíble un protocolo de enrutamiento entero en un único router. Cuanto menor es el número, mejor, o más creíble, es el protocolo de enrutamiento. Por ejemplo, RIP tiene un valor predeterminado de distancia administrativa de 120, y EIGRP un valor de 90, haciendo a EIGRP más creíble que RIP. Por tanto, cuando ambos protocolos de enrutamiento aprenden rutas a la misma subred, el router añade sólo la ruta de EIGRP a la tabla de enrutamiento.

Los valores de distancia administrativa se configuran en un único router y no se intercambia con otros routers. La Tabla 8.5 específica los distintos orígenes de la información de enrutamiento, junto con las distancias administrativas predeterminadas.

Tabla 8.5. Distancias administrativas predeterminadas.

Tipo de ruta	Distancia administrativa
Conectada	0
Estática	1
BGP (rutas externas)	20
EIGRP (rutas internas)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP (rutas externas)	170
BGP (rutas internas)	200
No utilizable	255

Nota

El comando `show ip route` muestra la distancia administrativa de cada ruta en el primero de los dos números entre corchetes. El segundo número es la métrica.

La tabla muestra los valores predeterminados de distancia administrativa, pero el IOS se puede configurar para cambiar la distancia administrativa de un protocolo de enrutamiento en concreto, una ruta determinada, e incluso una ruta estática. Por ejemplo, el comando `ip route 10.1.3.0 255.255.255.0 10.1.130.253` define una ruta estática con un valor predeterminado de distancia administrativa de 1, pero el comando `ip route 10.1.3.0 255.255.255.0 10.1.130.253 210` define la misma ruta estática con una distancia administrativa de 210.

Características del protocolo de enrutamiento por vector de distancia

Esta sección explica lo básico de los protocolos de enrutamiento por vector de distancia, utilizando RIP como ejemplo. Esta sección comienza examinando el funcionamiento

normal de los protocolos por vector de distancia, seguido de una explicación completa de muchas características del vector de distancia que permiten evitar los bucles.

El concepto de una distancia y un vector

El término **vector de distancia** describe qué conoce un router acerca de cada ruta. Al final del proceso, cuando un router aprende acerca de una ruta a una subred, todo lo que el router conoce es alguna medida de distancia (la métrica), el router de siguiente salto y la interfaz de salida a utilizar para esa ruta (un vector, o dirección). Para mostrar más exactamente lo que hace un protocolo por vector de distancia, la Figura 8.4 muestra una visión de qué aprende un router con un protocolo de enrutamiento por vector de distancia. La figura muestra una internetwork con R1 aprendiendo acerca de tres rutas para alcanzar la subred X:

- Ruta de cuatro saltos a través de R2.
- Ruta de tres saltos a través de R5.
- Ruta de dos saltos a través de R7.

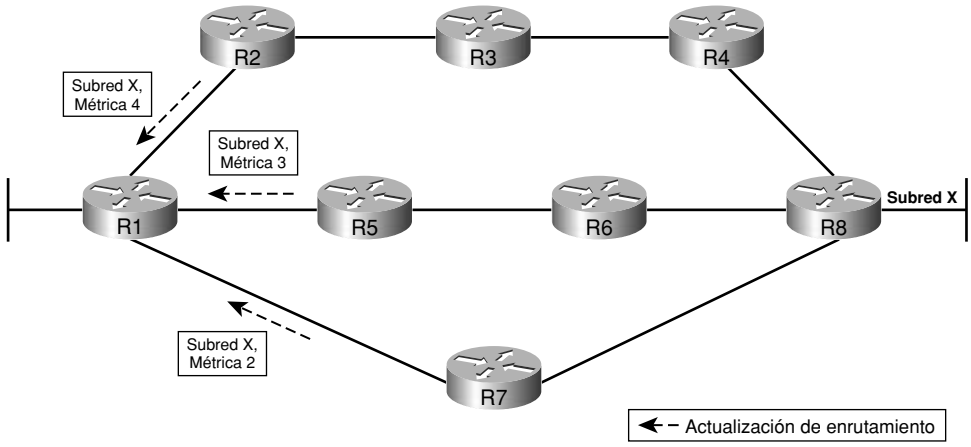


Figura 8.4. Información aprendida utilizando los protocolos por vector de distancia.

R1 aprende acerca de la subred, y una métrica asociada con esta subred, y nada más. R1 debe entonces elegir la mejor ruta para alcanzar la subred X. En este caso, elige la ruta de dos saltos a través de R7, porque esta ruta tiene la menor métrica. Para apreciar completamente el significado del término vector de distancia, considere la Figura 8.5, que muestra lo que R1 conoce realmente de la subred X de la Figura 8.4.

Efectivamente, todo lo que R1 conoce acerca de la subred X es tres vectores. La longitud de los vectores representa la métrica, que describe como de buena (o mala) es cada ruta. La dirección del vector representa el router de siguiente salto. Por tanto, con la lógica del vector de distancia, los protocolos de enrutamiento no aprenden mucho sobre la red cuando

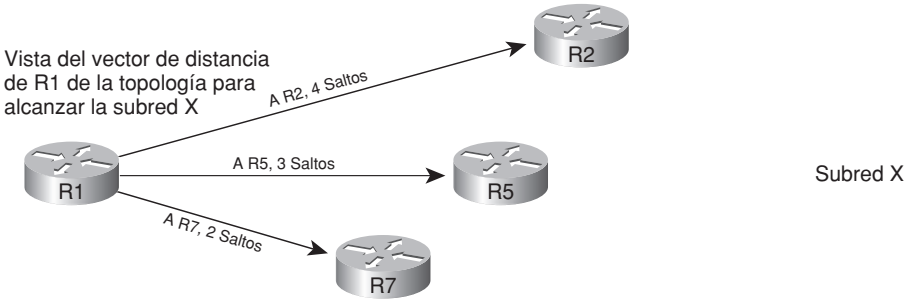


Figura 8.5. Representación gráfica del concepto de vector de distancia.

reciben las actualizaciones de enrutamiento. Todos los protocolos de enrutamiento conocen el mismo concepto de un vector: la longitud de un vector que es la distancia (métrica) para alcanzar una subred, y la dirección del vector que es el vecino a través del que se publica la ruta.

Funcionamiento del vector de distancia en una red estable

Los protocolos de enrutamiento por vector de distancia envían periódicamente actualizaciones de enrutamiento completas. La Figura 8.6 ilustra este concepto en una internetwork sencilla con dos routers, tres subredes LAN y otra subred WAN. La figura muestra las tablas de enrutamiento completas de los routers, listando las cuatro rutas, y las actualizaciones completas periódicas enviadas por cada router.

Para entender completamente el funcionamiento del vector de distancia en esta figura, nos centraremos en algunos de los hechos más importantes acerca de qué aprende el router R1 sobre la subred 172.30.22.0/24, que es la subred conectada a la interfaz Fa0/1 de R2:

1. R2 considera por sí mismo tener una ruta de 0 saltos para la subred 172.30.22.0/24; así, en la actualización de enrutamiento enviada por R2 (mostrada debajo del icono del router R2), R2 publica una ruta de métrica 1 (contador de salto 1).
2. R1 recibe la actualización RIP desde R2, y ya que R1 no ha aprendido otras posibles rutas para 172.30.22.0/24, esta ruta debe ser la mejor ruta de R1 hasta la subred.
3. R1 añade la subred a su tabla de enrutamiento, listándola como una ruta RIP aprendida.
4. Para la ruta aprendida, R1 utiliza una interfaz de salida de S0/0, porque R1 recibe una actualización de enrutamiento de R2 por la interfaz S0/0 de R1.
5. Para la ruta aprendida, R1 utiliza el router de siguiente salto 172.30.1.2, porque R1 aprende la ruta de una actualización RIP cuya dirección IP de origen era 172.30.1.2.

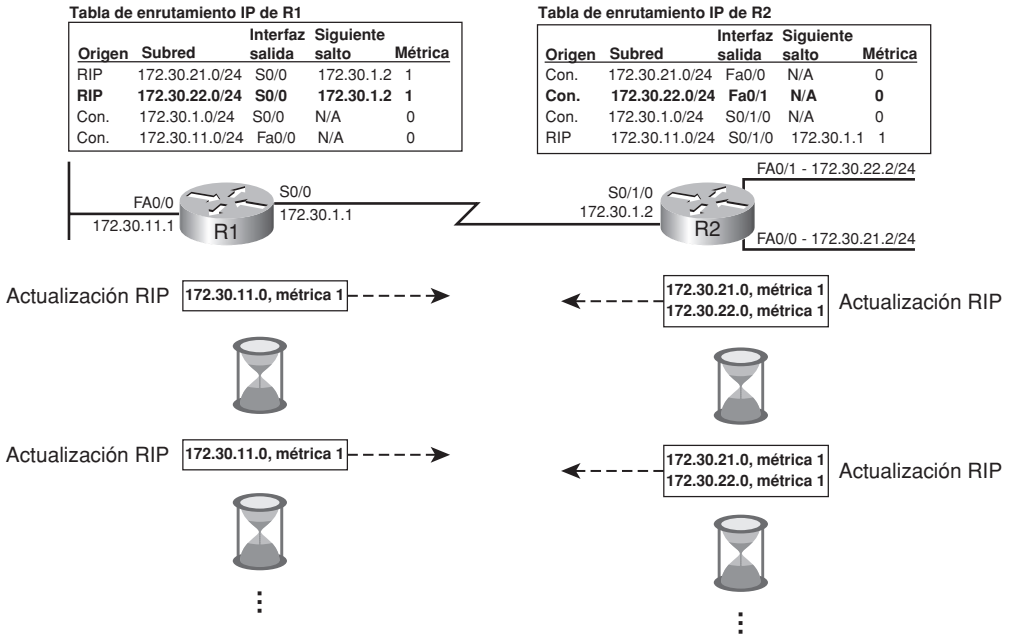


Figura 8.6. Funcionamiento de RIP en un estado estable normal.

Al final de este proceso, R1 ha aprendido una nueva ruta. El resto de las rutas RIP aprendidas en este ejemplo siguen el mismo proceso.

Además del proceso de publicación y aprendizaje de rutas, la Figura 8.6 también resalta unos pocos hechos particularmente importantes acerca de los protocolos por vector de distancia:

- **Periódicas:** El icono del reloj de arena representa el hecho de que las actualizaciones se repiten en un ciclo regular. RIP utiliza un intervalo de actualización predeterminado de 30 segundos.
- **Actualizaciones completas:** Los routers envían actualizaciones completas cada vez en lugar de enviar únicamente la información de enrutamiento nueva o que ha cambiado.
- **Actualizaciones completas limitadas por las reglas de horizonte dividido:** El protocolo de enrutamiento omite algunas rutas de las actualizaciones completas periódicas a causa de las reglas del horizonte dividido. El horizonte dividido es una característica de prevención de bucles que se trata en las próximas páginas.

Prevenir bucles del vector de distancia

Como se ha podido ver, el proceso real del vector de distancia es bastante simple. Desafortunadamente, la simplicidad de los protocolos por vector de distancia

introduce la posibilidad de bucles de enrutamiento. Los bucles de enrutamiento ocurren cuando los routers reenvían paquetes de modo que el mismo único paquete regresa a los mismos routers repetidamente, consumiendo ancho de banda y no entregando nunca el paquete. En las redes de producción, el número de paquetes en bucle puede congestionar la red hasta el punto de que la red llega a ser inutilizable; por tanto, los bucles de enrutamiento deben evitarse tanto como sea posible. El resto del tratamiento que este capítulo hace de los protocolos por vector de distancia se consagra a describir una variedad de características del vector de distancia que ayudan a prevenir los bucles.

Ruta envenenada

Cuando una ruta falla, en los protocolos de enrutamiento por vector de distancia hay riesgo de bucles de enrutamiento hasta que todos los routers de la internetwork creen y saben que la ruta original ha fallado. Como resultado, los protocolos por vector de distancia necesitan una forma de identificar específicamente qué rutas han fallado.

Los protocolos por vector de distancia extienden las malas noticias acerca de la ruta fallida envenenando la ruta. El **envenenamiento de ruta** se refiere a la práctica de publicar una ruta, pero con un valor de métrica especial llamada **infinito**. Simplemente, los routers consideran que las rutas publicadas con esta métrica han fallado. Observe que cada protocolo de enrutamiento por vector de distancia utiliza el concepto de un valor de métrica actual que representa infinito. RIP define infinito como 16.

La Figura 8.7. muestra un ejemplo de ruta envenenada con RIP, con la interfaz Fa0/1 de R2 fallando, lo que significa que la ruta de R2 para 172.30.22.0/24 ha fallado.

Nota

Aunque las rutas envenenadas por RIP tienen una métrica de 16, el comando show ip route no muestra el valor de la métrica. En cambio, muestra la frase *"possibly down"*.

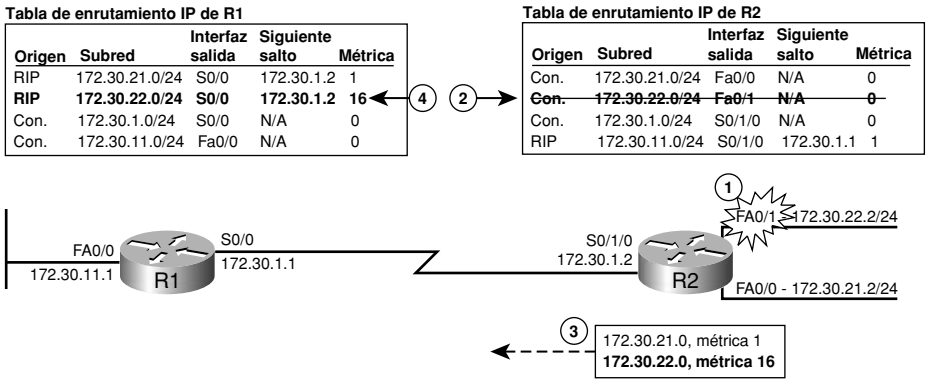


Figura 8.7. Ruta envenenada.

La Figura 8.7. muestra el siguiente proceso:

1. La interfaz Fa0/1 de R2 falla.
2. R2 elimina su ruta conectada para 172.30.22.0/24 de su tabla de enrutamiento.
3. R2 publica 172.30.22.0 con una métrica infinita, que para RIP es una métrica de 16.
4. R1 mantiene la ruta en su tabla de enrutamiento, con una métrica infinita, hasta que elimina la ruta de la tabla de enrutamiento.

Cualquier valor de métrica menor que infinito se puede utilizar como una métrica válida para una ruta válida. Con RIP, esto significa que una ruta a 15 saltos podría ser una ruta válida. Algunas de las grandes redes empresariales en el mundo tienen al menos cuatro o cinco routers en la ruta más larga entre cualesquiera dos subredes; por tanto, una métrica máxima de 15 saltos es suficiente.

Problema: cuenta hasta infinito en un único enlace

Los protocolos de enrutamiento por vector de distancia introducen el riesgo de que se formen bucles de enrutamiento durante el tiempo entre que el primer router comprende que ha fallado una ruta hasta que todos los routers saben que la ruta ha fallado. Sin los mecanismos de prevención de bucles examinados en este capítulo, los protocolos por vector de distancia pueden experimentar un problema llamado cuenta hasta infinito. Ciertamente, los routers no pueden nunca contar literalmente hasta infinito, pero pueden contar hasta su versión de infinito; por ejemplo, hasta 16 en RIP.

El recuento hasta infinito causa dos problemas relacionados. Varias de las características de prevención de bucles del vector de distancia se centran en prevenir estos problemas:

- Los paquetes pueden formar bucles alrededor de la internetwork mientras los routers cuentan hasta infinito, con el ancho de banda consumido por los paquetes en bucle paralizando la internetwork.
- El proceso de contar hasta infinito puede llevar varios minutos, de modo que el bucle puede hacer pensar a los usuarios que la red falla.

Cuando los routers cuentan hasta infinito, colectivamente van cambiando su idea sobre la métrica de una ruta fallida. La métrica crece despacio hasta que alcanza el infinito, momento en que los routers finalmente creen que la ruta ha fallado. La mejor manera de entender este concepto es con un ejemplo; la Figura 8.8 muestra el comienzo del problema del recuento hasta infinito.

La clave de estos ejemplos es conocer que las actualizaciones periódicas de R1a R2 (de izquierda a derecha en la Figura 8.8) ocurren aproximadamente en el mismo instante que la publicación de ruta envenenada de R2 a R1. La Figura 8.8 muestra el siguiente proceso:

1. La interfaz Fa0/1 de R2 falla, por lo que R2 elimina su ruta conectada para 172.30.22.0/24 de su tabla de enrutamiento.
2. R2 envía una publicación de ruta envenenada (métrica 16 para RIP) a R1, pero **aproximadamente al mismo tiempo**, el temporizador de actualizaciones periódicas de R1 expira, por lo que R1 envía su actualización regular, incluyendo una publicación sobre 172.30.22.0, métrica 2.

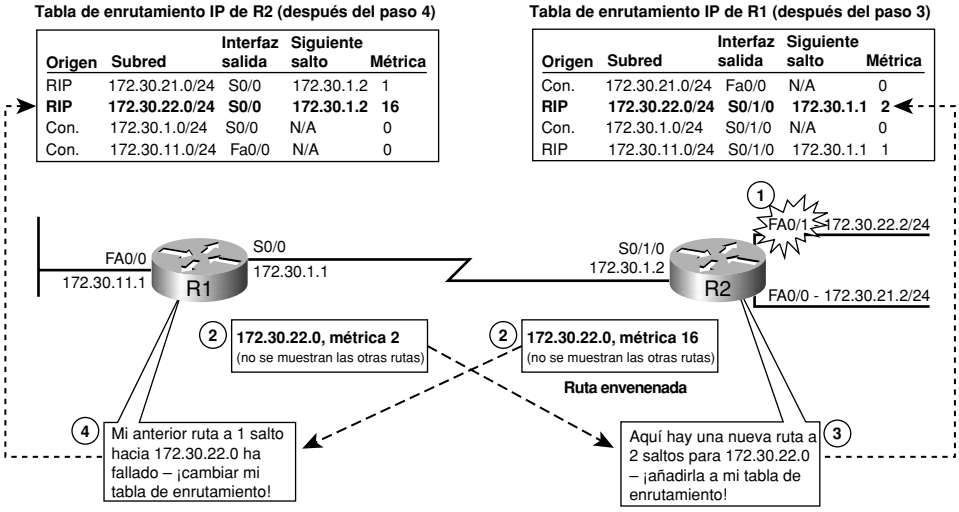


Figura 8.8. R2 cree incorrectamente que R1 tiene una ruta a 172.16.22.0/24.

3. R2 escucha esta ruta de métrica 2 para alcanzar 172.30.22.0 desde R1. Ya que R2 no tiene una ruta para la subred 172.30.22.0, añade la ruta a dos saltos a su tabla de enrutamiento con R1 como router de siguiente salto.
4. Aproximadamente al mismo tiempo que el Paso 3, R1 recibe la actualización desde R2, diciendo a R1 que su ruta anterior a 172.30.22.0, a través de R2, ha fallado. Como resultado, R1 cambia su tabla de enrutamiento para especificar una métrica de 16 para la ruta hacia 172.30.22.0.

En este punto, R1 y R2 reenvían paquetes destinados a 172.30.22.0/24 de atrás para adelante entre sí. R2 tiene una ruta para 172.30.22.0/24, apuntando a R1, y R1 tiene la inversa. El bucle ocurre entre R1 y R2 porque ambos cuentan hasta infinito. La Figura 8.9 muestra el siguiente paso en su marcha cooperativa hasta el infinito.

La Figura 8.9 muestra las siguientes actualizaciones periódicas de ambos routers, como sigue:

1. Los temporizadores de actualizaciones de R1 y R2 expiran aproximadamente al mismo tiempo. R1 publica una ruta envenenada (métrica 16), y R2 publica una ruta de métrica 3. (Recuerde, los routers RIP añaden 1 a la métrica antes de publicar la ruta.)
2. R2 recibe la actualización de R1; por tanto, R2 cambia su ruta para 172.30.22.0 a una métrica de 16.
3. Aproximadamente al mismo tiempo que el Paso 2, R1 recibe la actualización de R2; así, R1 cambia su ruta para 172.30.22.0 a una métrica de 3.

El proceso continúa por cada ciclo de actualización periódico, con ambos routers alcanzando eventualmente la métrica 16. En este punto, los routers pueden eliminar la ruta de sus tablas de enrutamiento.

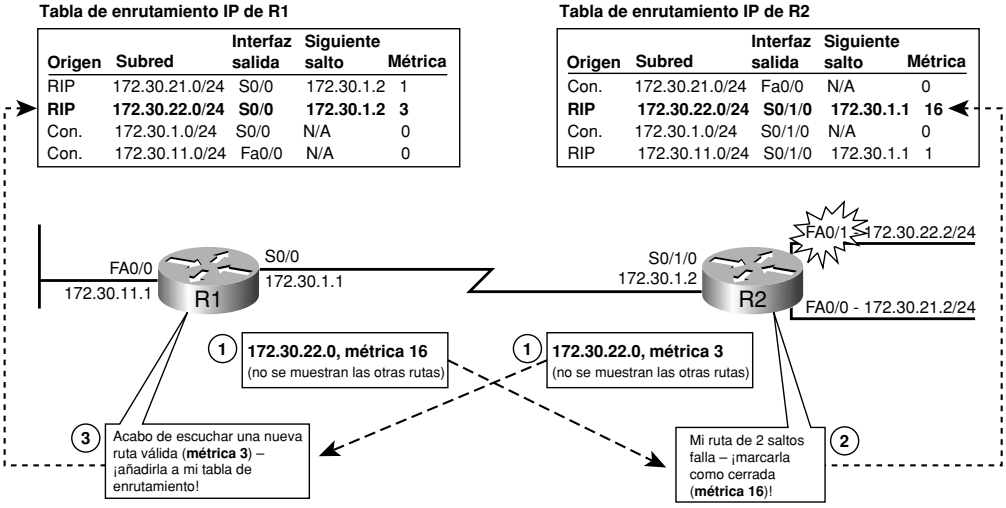


Figura 8.9. R1 y R2 contando hasta infinito.

Horizonte dividido

En la internetwork sencilla utilizada en las Figuras 8.8 y 8.9, el router R2 tiene una ruta conectada a 172.30.22.0, y R1 aprende la ruta porque R2 envía una actualización de enrutamiento. Sin embargo, hay una pequeña necesidad por parte de R1 de publicar esta misma ruta de vuelta a R2, porque R1 aprendió esta ruta de R2 en primer lugar. Por tanto, una manera de prevenir el problema del recuento hasta infinito mostrado en estas figuras es que R1 simplemente no publique la subred 172.30.22.0, usando una característica llamada horizonte dividido. El horizonte dividido se define como sigue:

Tema clave

> En las actualizaciones de enrutamiento enviadas por la interfaz X, no incluir la información de enrutamiento acerca de las rutas que se refieran a la interfaz X como interfaz de salida.

Los protocolos por vector de distancia funcionan en cierta forma como los rumores entre las personas de una comunidad de vecinos. La gente habla con sus vecinos, que se lo dicen a otros vecinos, hasta que finalmente todo el vecindario se entera del último chisme. Siguiendo esta analogía, si oye un rumor de su vecino Fred, usted no se da la vuelta y le cuenta a él el mismo rumor. Asimismo, el horizonte dividido significa que cuando el router R1 aprende una ruta desde el router R2, R1 no tiene necesidad de publicar la misma ruta de vuelta a R2.

La Figura 8.10 muestra el efecto del horizonte dividido en los routers R1 y R2 en la misma internetwork ya familiar. La tabla de enrutamiento de R1 (en la parte superior de la figura) lista cuatro rutas, tres de las cuales tienen a la interfaz S0/0 de R1 como interfaz de salida. Por tanto, el horizonte dividido impide a R1 incluir estas tres rutas en la actualización enviada por R1 de salida por su interfaz S0/0.

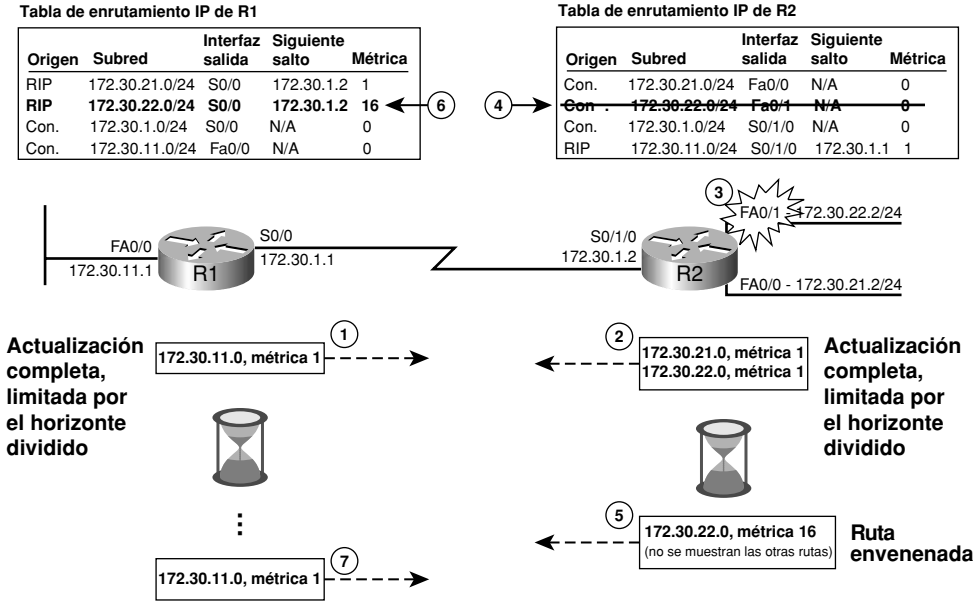


Figura 8.10. Efectos del horizonte dividido sin invertir envenenada.

La Figura 8.10 muestra el siguiente proceso:

1. R1 envía su actualización completa periódica normal, que, debido a las reglas del horizonte dividido, incluye sólo una ruta.
2. R2 envía su actualización completa periódica normal, que, debido a las reglas del horizonte dividido, incluye sólo dos rutas.
3. La interfaz Fa0/1 de R2 falla.
4. R2 elimina su ruta conectada para 172.30.22.0/24 de su tabla de enrutamiento.
5. R2 publica 172.30.22.0 con una métrica infinita, que en RIP es una métrica de 16.
6. R1 mantiene temporalmente la ruta para 172.30.22.0 en su tabla de enrutamiento; después, elimina la ruta de la tabla de enrutamiento.
7. En su siguiente actualización regular, R1, debido al horizonte dividido, todavía no publica la ruta para 172.30.22.0.

El horizonte dividido previene el problema del recuento hasta infinito mostrado en las Figuras 8.8 y 8.9, ya que R1 no publica 172.30.22.0 a R2 en absoluto. Como resultado, R2 nunca oye nada acerca de una ruta alternativa (incorrecta) hacia 172.30.22.0. El IOS de Cisco utiliza de forma predeterminada el horizonte dividido en la mayoría de las interfaces.

Nota

La implementación RIP con el IOS de Cisco no actúa exactamente como se ha descrito en el Paso 7 de este particular ejemplo. En cambio, utiliza una característica llamada inversa envenenada, como se describe en la siguiente sección.

Inversa envenenada y actualizaciones Activadas

Los protocolos por vector de distancia pueden atajar el problema del recuento hasta infinito asegurándose de que todo router aprende que la ruta ha fallado, a través de todos los medios posibles, tan rápidamente como sea posible. Las dos características siguientes de prevención de bucles hacen justo esto y se definen como sigue:

- **Actualizaciones activadas:** Cuando una ruta falla, no espera a la siguiente actualización periódica. En cambio, envía inmediatamente una actualización activada que especifica la ruta envenenada.
- **Inversa envenenada:** Cuando se aprende una ruta fallida, suspender las reglas del horizonte dividido para esta ruta, y publicar una ruta envenenada.

La Figura 8.11 muestra un ejemplo de cada una de estas características, con la interfaz Fa0/1 de R2 fallando una vez más. Observe que la figura comienza con todas las interfaces funcionando, y todas las rutas conocidas.

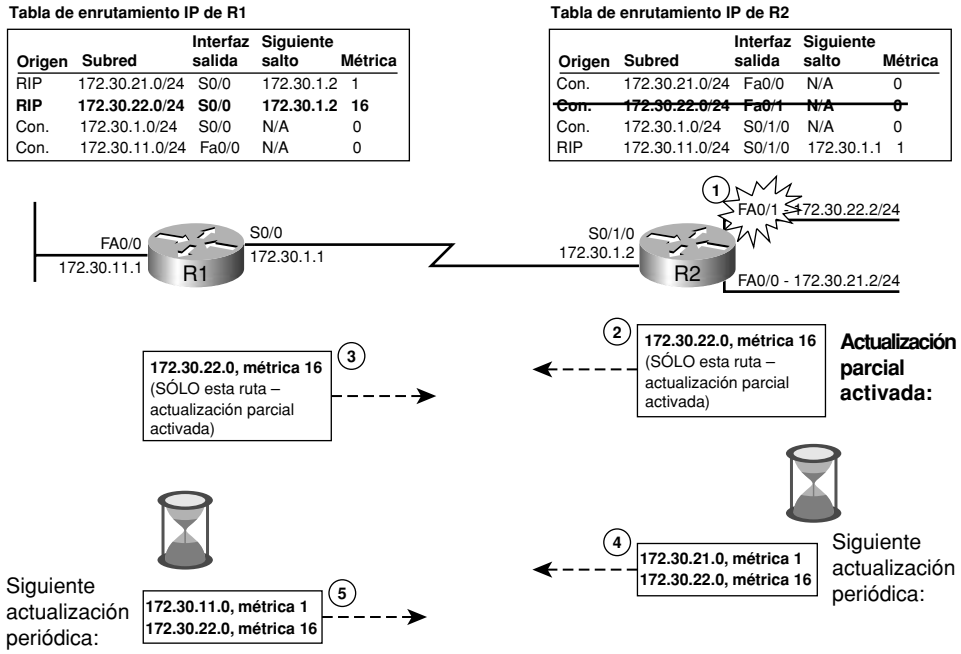


Figura 8.11. R2 enviando una actualización activada, con R1 publicando una ruta inversa envenenada.

El proceso mostrado en la Figura 8.11 se ejecuta como sigue:

1. La interfaz Fa0/1 de R2 falla.
2. R2 envía inmediatamente una actualización parcial activada con sólo la información que ha cambiado; en este caso, una ruta envenenada para 172.30.22.0.

3. R1 responde cambiando su tabla de enrutamiento y enviando inmediatamente de vuelta una actualización parcial (activada), listando sólo 172.30.22.0 con una métrica infinita (métrica 16). Esto es una ruta inversa envenenada.
4. En la siguiente actualización periódica regular de R2, R2 publica por un tiempo todas las rutas típicas, incluyendo la ruta envenenada para 172.30.22.0.
5. En la siguiente actualización periódica regular de R1, R1 publica por un tiempo todas las rutas típicas, más la ruta inversa envenenada para 172.30.22.0.

En este ejemplo, R2 reacciona inmediatamente enviando la actualización activada. R1 también reacciona inmediatamente, suspendiendo las reglas del horizonte dividido para la ruta fallida para enviar una ruta inversa envenenada. De hecho, la ruta envenenada de R2 no se considera una ruta inversa envenenada, porque R2 ya publicó una ruta para 172.30.22.0. Sin embargo, la ruta envenenada de R1 es una ruta inversa envenenada porque fue publicada de vuelta al router del que R1 aprendió acerca de la ruta fallida. De hecho, algunos libros también se refieren a la inversa envenenada como **horizonte dividido con inversa envenenada**, porque el router suspende la regla de horizonte dividido para la ruta fallida.

Problema: cuenta hasta infinito en una red redundante

El horizonte dividido evita que el problema del recuento hasta infinito tenga lugar entre dos routers. Sin embargo, con rutas redundantes en una internetwork, lo que es común en la mayoría de las internetworks actuales, el horizonte dividido por sí sólo no previene el problema del recuento hasta infinito. Para ver el problema, la Figura 8.12 muestra la nueva red funcionando en su estado normal, estable y todo operativo. Las Figuras 8.13 y 8.14 muestran un momento en el que se produce un recuento hasta infinito, incluso con el horizonte dividido habilitado.

Nota

La Figura 8.12 omite las actualizaciones RIP que podrían ser enviadas por las interfaces LAN para hacer la figura menos liosa.

Además de mostrar el funcionamiento normal de otra red, la Figura 8.12 proporciona un buen ejemplo de cómo funciona el horizonte dividido. De nuevo utilizando la subred 172.30.22.0 como un ejemplo, el siguiente proceso ocurre en esta internetwork:

1. R2 publica una ruta de métrica 1 en su actualización para R1 y R3.
2. R1 entonces publica una ruta de métrica 2 para 172.30.22.0 a R3, y R3 publica una ruta de métrica 2 para 172.30.22.0 a R2.
3. R1 y R3 añaden la ruta de métrica 1, aprendida directamente de R2, a sus tablas de enrutamiento, e ignoran las rutas a dos saltos que aprenden uno del otro. Por ejemplo, R1 anota la ruta a 172.30.22.0, usando la interfaz de salida S0/0, router de siguiente salto 172.30.1.2 (R2), en su tabla de enrutamiento.

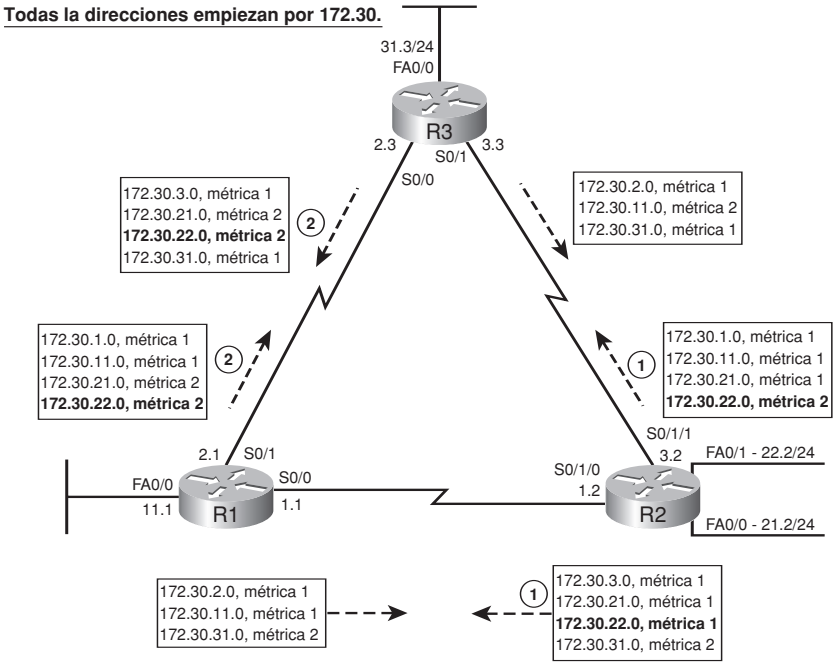


Figura 8.12. Actualización periódica en una internetwork triangular estable.

El horizonte dividido impide a R1 y R3 publicar la subred 172.30.22.0 de vuelta a R2. Observe que la Figura 8.12 muestra todas las publicaciones de ruta para 172.30.22.0 en negrita. R1 y R3 no listan a 172.30.22.0 en sus actualizaciones enviadas de vuelta a R2. De hecho, todas las actualizaciones de enrutamiento que se muestran en la Figura 8.12 presentan los efectos del horizonte dividido.

Ahora que se ha entendido bien la internetwork mostrada en la Figura 8.12, la Figura 8.13 muestra la misma internetwork, pero con el comienzo del problema del recuento hasta infinito, aunque el horizonte dividido está habilitado. De nuevo, Fa0/1 de R2 comienza el ejemplo fallando.

El proceso mostrado en la Figura 8.13 es como sigue. Como es habitual, este ejemplo detalla algún desafortunado momento en el que las actualizaciones de enrutamiento periódicas se realizan en aproximadamente el mismo momento en que una ruta falla.

1. La interfaz Fa0/1 de R2 falla.
2. R2 envía inmediatamente una actualización parcial activada, envenenando la ruta para 172.30.22.0. R2 envía las actualizaciones por todas las interfaces que todavía funcionan.
3. R3 recibe la actualización activada de R2 que envenena la ruta para 172.30.22.0; por tanto, R3 actualiza su tabla de enrutamiento para especificar la métrica 16 para esta ruta.

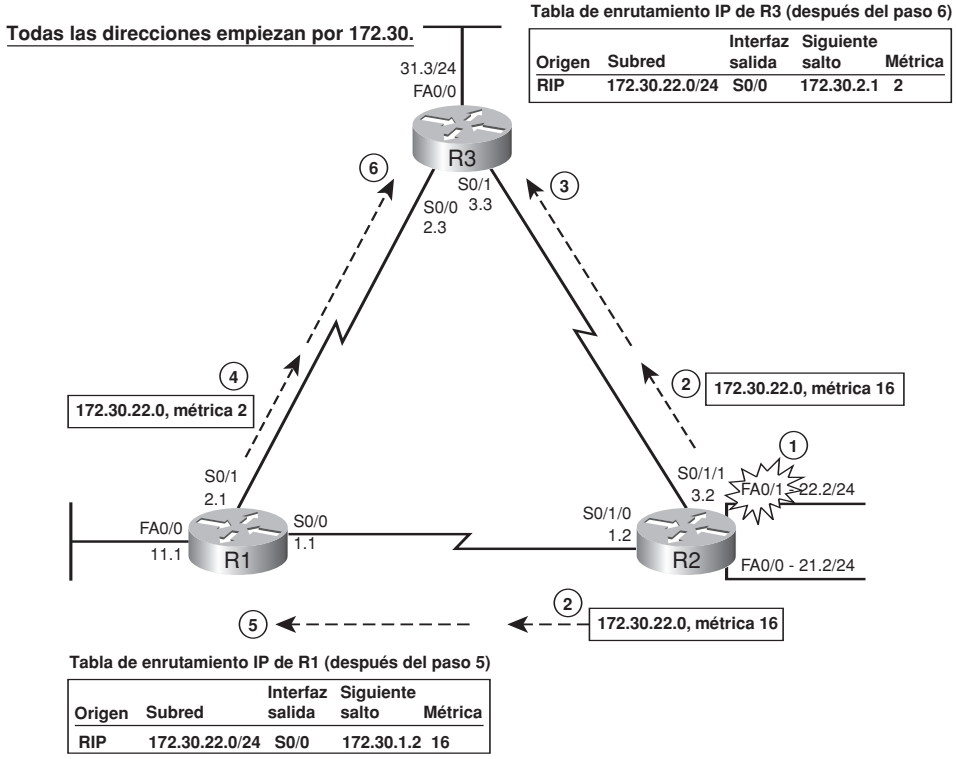


Figura 8.13. Recuento hasta Infinito en una internetwork redundante.

4. Antes de que la actualización descrita en el Paso 2 llegue a R1, R1 envía sus actualizaciones periódicas normales a R3, especificando 172.30.22.0, métrica 2, como normal. (Observe que la Figura 8.13 omite algo de lo que iría en la actualización periódica de R1 para reducir el conjunto.)
5. R1 recibe la actualización activada de R2 (descrita en el Paso 2) que envenena la ruta para 172.30.22.0; así, R1 actualiza su tabla de enrutamiento para especificar la métrica 16 para esta ruta.
6. R3 recibe la actualización periódica enviada por R1 (descrita en el Paso 4), especificando una ruta de métrica 2 para 172.30.22.0. Como resultado, R3 actualiza su tabla de enrutamiento para listar una ruta de métrica 2, a través de R1 como el router de siguiente salto, con la interfaz de salida S0/0.

En este punto, R3 tiene una ruta incorrecta de métrica 2 para 172.30.22.0, apuntando de regreso a R1. Dependiendo del momento en que la entrada llegue y deje la tabla de enrutamiento, los routers podrían terminar reenviando los paquetes enviados a la subred 172.30.22.0/24 a través de la red, posiblemente con algunos paquetes entrando en bucle varias veces, mientras el proceso de cuenta hasta infinito continúa.

El proceso y el temporizador *holddown*

La última característica de prevención de bucles tratada en este capítulo, un proceso llamado ***holddown***, previene los bucles y el problema de la cuenta hasta infinito mostrado en la Figura 8.13. Los protocolos por vector de distancia utiliza el *holddown* para prevenir especialmente los bucles creados por el problema del recuento hasta infinito que surgen en las internetworks redundantes. El término *holddown* da una idea de su significado:

> Tan pronto como la ruta falla, **matenerla desactivada (*holddown*) mientras** se da tiempo a los routers para estar seguros de que todo router sabe que la ruta ha fallado.

El proceso de *holddown* le dice a un router que ignore la nueva información acerca de la ruta que falla, por un tiempo denominado tiempo *holddown*, que se contabiliza utilizando el ***temporizador holddown***. El proceso *holddown* puede resumirse como sigue:

Tema clave

> Después de escuchar una ruta envenenada, se inicia un temporizador *holddown* para esa ruta. Hasta que el temporizador expire, no se cree en producir cualquier otra información acerca de la ruta fallida, porque creyendo esta información se pueden producir bucles de enrutamiento. Sin embargo, la información aprendida del vecino que originalmente publicó la ruta cuando funcionaba puede ser creída antes de que el temporizador expire.

El concepto *holddown* se entiende mejor con un ejemplo. La Figura 8.14 repite el ejemplo de la Figura 8.13, pero con el proceso *holddown* de R3 previniendo el problema del recuento hasta infinito. La figura muestra cómo R3 ignora cualquier nueva información sobre la subred 172.30.22.0 debido al estado *holddown*. Como es habitual, la figura comienza con todas las interfaces activas y funcionando, y todas las rutas conocidas, y con el fallo de la misma interfaz del router R2 en el Paso 1.

El proceso mostrado en la Figura 8.14 es como sigue, con los Pasos 3 y 6 diferentes de los pasos de la Figura 8.13:

1. La interfaz Fa0/1 de R2 falla.
2. R2 envía inmediatamente una actualización parcial activada, envenenando la ruta para 172.30.22.0. R2 envía la actualización por las interfaces que todavía funcionan.
3. R3 recibe la actualización activada de R2 que envenena la ruta para 172.30.22.0, de modo que R3 actualiza su tabla de enrutamiento para listar la métrica 16 para esta ruta. R3 también coloca la ruta para 172.30.22.0 en *holddown* e inicia el temporizador *holddown* para la ruta (el valor predeterminado para RIP es de 180 segundos).
4. Antes de que la actualización descrita en el Paso 2 llegue a R1, R1 envía su actualización periódica normal a R3, especificando 172.30.22.0, métrica 2, como normal. (Observe que la Figura 8.14 omite algunos detalles en la actualización periódica de R1 para simplificarla.)

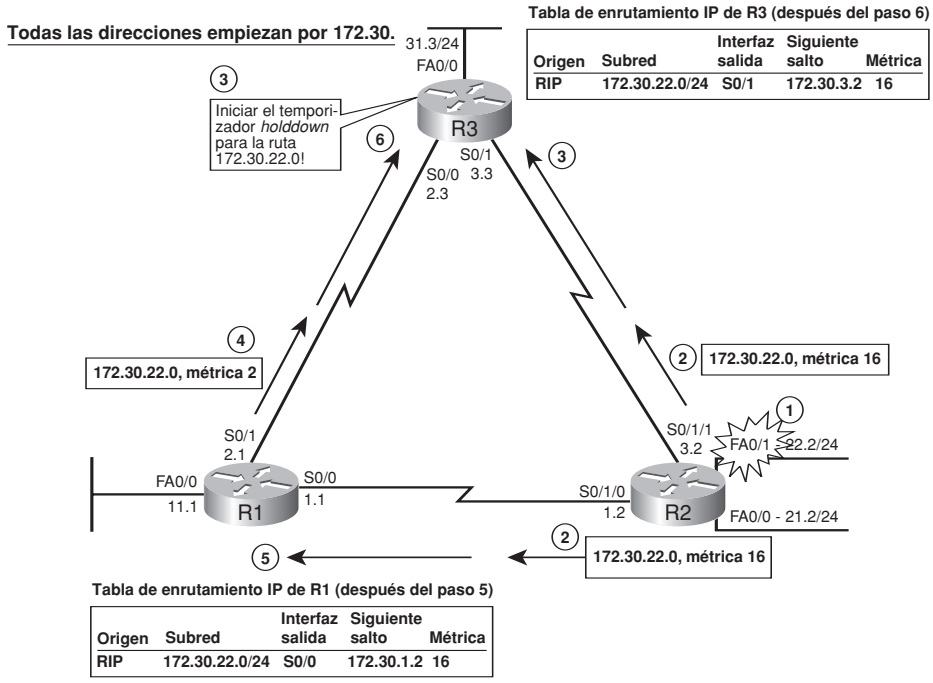


Figura 8.14. Uso de *holddown* para prevenir la cuenta hasta infinito.

5. R1 recibe la actualización activada de R2 (descrita en el Paso 2) que envenena la ruta para 172.30.22.0, de modo que R1 actualiza su tabla de enrutamiento para especificar la métrica 16 para esta ruta.
6. R3 recibe la actualización desde R1 (descrito en el Paso 4), listando una ruta de métrica 2 para 172.30.22.0. Como R3 ha colocado esta ruta en un estado *holddown*, y esta nueva ruta de métrica 2 fue aprendida de un router diferente (R1) del de la ruta original (R2), R3 ignora la nueva información de enrutamiento.

Como resultado de la lógica *holddown* de R3 descrita en el Paso 6, los tres routers tienen una ruta de métrica 16 para 172.30.22.0. En este punto, cualesquiera actualizaciones de enrutamiento futuras listarán sólo las rutas de métrica 16 para esta subred (al menos hasta que una ruta real a la subred funcione de nuevo).

La definición de *holddown* permite a los routers creer al mismo router que originalmente publicó la ruta, incluso antes de que el temporizador *holddown* expire. Por ejemplo, el proceso entero de la Figura 8.14 puede suceder en unos pocos segundos debido a todas las actualizaciones activadas. Si la interfaz Fa0/1 de R2 se vuelve a activar, R2 entonces publica una ruta de métrica 1 para 172.30.22.0 de nuevo. Si R1 y R3 creyeran las publicaciones de R2, podrían evitar la espera de más de 3 minutos para que sus temporizadores *holddown* expiren para la subred 172.30.22.0. Creyendo la actualización de enrutamiento desde el mismo router que originalmente publicó la ruta no se arriesga a provocar un bucle. Por

tanto, permanecer *holddown* permite a los routers (en este caso R1 y R3) creer en las publicaciones de R2.

Resumen del vector de distancia

Antes de cerrar el tratamiento de la prevención de bucles en el vector de distancia, es útil revisar los conceptos aquí tratados. Esta sección ha tratado mucha teoría, parte de la cual puede ser un poco engañosa, pero las principales características se resumen fácilmente:

- Durante los periodos de estabilidad, los routers envían actualizaciones de enrutamiento periódicas completas basándose en un corto temporizador de actualizaciones (en RIP el valor predeterminado es 30 segundos). Las actualizaciones listan todas las rutas conocidas excepto las rutas omitidas por la aplicación de las reglas del horizonte dividido.
- Cuando ocurren cambios que causan que una ruta falle, el router que advierte el fallo reacciona inmediatamente enviando una actualización parcial activada, listando sólo las rutas nuevamente envenenadas (fallidas), con una métrica infinita.
- Otros routers que escuchan la ruta envenenada también envían actualizaciones parciales activadas, envenenando la ruta fallida.
- Los routers suspenden sus reglas de horizonte dividido para la ruta fallida enviando una ruta inversa envenenada de vuelta al router desde el cual la ruta envenenada fue aprendida.
- Todos los routers colocan la ruta en el estado *holddown* y se inicia el temporizador *holddown* para esta ruta después de aprender que la ruta ha fallado. Cada router ignora toda nueva información acerca de esta ruta hasta que el temporizador *holddown* expira, a menos que esta información proceda del mismo router que originalmente publicó la ruta buena para esta subred.

Características del protocolo de enrutamiento por estado del enlace

Al igual que los protocolos por vector de distancia, los protocolos por estado del enlace envían actualizaciones de enrutamiento a los routers vecinos, los cuales a su vez envían sus actualizaciones a sus routers vecinos, y así sucesivamente. Al final del proceso, igual que los protocolos por vector de distancia, los routers que utilizan los protocolos por estado del enlace añaden las mejores rutas a sus tablas de enrutamiento, basándose en las métricas. Sin embargo, más allá de este nivel de explicación, estos dos tipos de algoritmos de protocolo de enrutamiento tienen poco en común.

Esta sección trata la mayoría de los mecanismos básicos de cómo funcionan los protocolos por estado del enlace, utilizando en los ejemplos Primero la ruta libre más corta

(OSPF, *Open Shortest Path First*), el primer protocolo de enrutamiento IP por estado del enlace. Esta sección comienza mostrando cómo los protocolos de enrutamiento por estado del enlace inundan la información de enrutamiento a través de la internetwork. Después se describe cómo los protocolos por estado del enlace procesan la información de enrutamiento para elegir las mejores rutas.

Construyendo la misma LSDB en todos los routers

Los routers que utilizan los protocolos de enrutamiento por estado del enlace necesitan publicar colectivamente prácticamente todos los detalles acerca de la internetwork a todos los otros routers. Al final del proceso, llamado inundación, todo router de la internetwork tiene exactamente la misma información acerca de la misma. Los routers utilizan esta información, almacenada en la RAM en una estructura de datos llamada base de datos de estado del enlace (LSDB), para realizar el otro proceso principal del estado del enlace para calcular las mejores rutas actuales a cada subred. Inundar toda la información detallada a todos los routers parece mucho trabajo, y respecto a los protocolos de enrutamiento por vector de distancia, lo es.

Primero la ruta libre más corta (OSPF), el protocolo más extendido de enrutamiento IP por estado del enlace, publica información en los mensajes de actualización de enrutamiento de varios tipos; estas actualizaciones contienen información denominada publicación de estado del enlace (LSA). Las LSAs llegan en muchas formas, incluyendo los siguientes tipos principales:

- **LSA de router:** Incluye un número de identidad del router (ID de router), las direcciones IP y las máscaras de la interfaz del router, el estado (*up* o *down*) de cada interfaz, y el coste (métrica) asociado con la interfaz.
- **LSA de enlace:** Identifica cada enlace (subred) y los routers que están conectados a este enlace. También se identifica el estado del enlace (*up* o *down*).

Algunos routers deben crear primero las LSAs de router y de enlace, y entonces inundar las LSAs a todos los otros routers. Cada router crea una LSA de router para sí mismo y entonces inunda esta LSA a otros routers en mensajes de actualización de enrutamiento. Para inundar una LSA, un router envía la LSA a sus vecinos. Estos vecinos a su vez reenvían la LSA a sus vecinos, y así sucesivamente, hasta que todos los routers han aprendido acerca de la LSA. Para las LSAs de enlace, un router conectado a una subred también crea e inunda una LSA de enlace para cada subred. (Observe que en algunos casos no se necesita una LSA de enlace, normalmente cuando sólo un router conecta con la subred.) Al final del proceso, todos los routers tienen todas las LSA de router de los otros routers y una copia de todas las LSAs de enlace también.

La Figura 8.15 muestra la idea general del proceso de inundación, con R8 creando y difundiendo su LSA de router. Observe que la Figura 8.15 realmente muestra sólo un subconjunto de la información disponible en la LSA de router de R8.

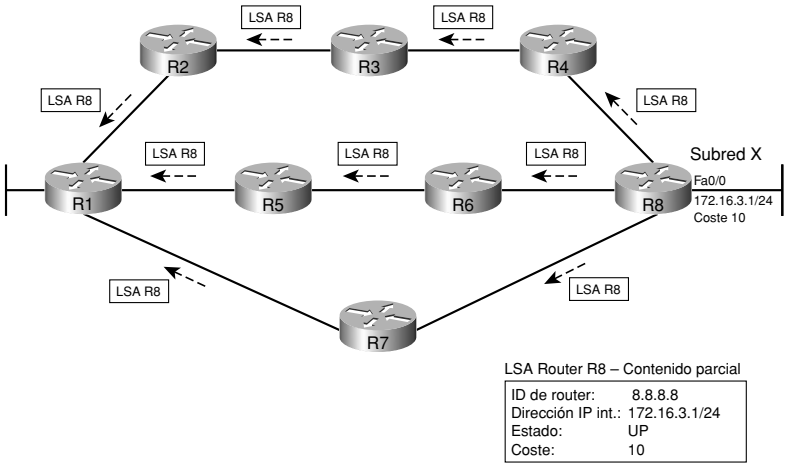


Figura 8.15. Inundando LSAs utilizando un protocolo de enrutamiento por estado del enlace.

La Figura 8.15 muestra el proceso básico de inundación, con R8 enviando la LSA original para sí mismo, y los otros routers inundando la LSA reenviándola hasta que cada router tenga una copia. Para evitar bucles en las publicaciones de LSA, un router que recibe una LSA primero pregunta a sus vecinos si ya conocen esa LSA. Por ejemplo, R8 podría comenzar preguntando por separado a R4, R6 y R7 si ellos conocen la LSA de router para R8. Estos tres routers podrían contestar, declarando que ellos no conocen a la LSA de router de R8. Sólo en este punto R8 envía la LSA a cada uno de estos routers vecinos. El proceso se repite con todos los vecinos. Si un router ya ha aprendido la LSA —no importa por que camino— él puede políticamente decir que ya tiene la LSA, así se previene que la LSA anunciada forme un bucle alrededor de la red.

El origen del término **estado del enlace** puede explicarse considerando el contenido (parcial) de la LSA de router que se muestra en la Figura 8.15. La figura muestra una de las cuatro direcciones IP de interfaz que podría ser especificada en la LSA de router del router R8, junto con el estado de la interfaz. Los protocolos por estado del enlace obtienen su nombre del hecho de que las LSAs publican cada interfaz (enlace) y si la interfaz está *up* o *down* (estado). Por tanto, la LSDB contiene información acerca de no sólo los routers e interfaces y enlaces (subredes) activos y funcionando, sino de todos los routers e interfaces y enlaces (subredes), incluso si las interfaces están inactivas.

Después de que la LSA haya sido inundada, incluso si las LSAs no han cambiado, los protocolos por estado del enlace necesitan de reinundaciones periódicas de las LSAs, similar a las actualizaciones periódicas enviadas por los protocolos por vector de distancia. Sin embargo, los protocolos por vector de distancia típicamente utilizan un tiempo corto; por ejemplo, RIP envía actualizaciones periódicas cada 30 segundos y RIP envía una actualización completa listando normalmente todas las rutas publicadas. OSPF reinunda cada LSA basándose en el temporizador de edad separado de cada LSA (de forma predeterminada cada 30 minutos). Como resultado, en una red estable, los protocolos por estado del enla-

ce realmente utilizan menos ancho de banda para enviar la información de enrutamiento que los protocolos por vector de distancia. Si una LSA cambia, el router inmediatamente inunda la LSA modificada. Por ejemplo, si falla la interfaz LAN del router de la Figura 8.15, R8 podría necesitar reinundar la LSA de R8, declarando que la interfaz está ahora desactivada.

Aplicando la matemática SPF de Dijkstra para encontrar las mejores rutas

El proceso de inundación del estado del enlace finaliza con todos los routers teniendo una copia idéntica de la LSDB en memoria, pero el proceso de inundación sólo no provoca que un router aprenda qué rutas añadir a la tabla de enrutamiento IP. Aunque increíblemente detallada y útil, la información de la LSDB no declara explícitamele la mejor ruta de cada router hacia un destino. Los protocolos por estado del enlace deben utilizar otra parte principal del algoritmo del estado del enlace para encontrar y añadir rutas a la tabla de enrutamiento IP: las rutas que muestran un número de subred y una máscara, una interfaz de salida, y la dirección IP del router de siguiente salto. Este proceso utiliza algo llamado algoritmo SPF (Primero la ruta más corta, *Shortest Path First*) de Dijkstra.

El algoritmo SPF se puede comparar a como los humanos piensan cuando realizan un viaje utilizando un mapa de carreteras. Cualquiera puede comprar el mismo mapa de carreteras; por tanto, cualquiera puede conocer la información acerca de las carreteras. Sin embargo, cuando se mira un mapa, primero se localizan los puntos inicial y final, y después se analiza el mapa para encontrar posibles rutas. Si varias rutas parecen similares en longitud, se puede decidir tomar una ruta más larga si las carreteras son autopistas en lugar de carreteras nacionales. Cualquier otro con el mismo mapa, puede comenzar en un lugar diferente, y desear ir a otro sitio; por tanto, puede elegir tomar una ruta completamente diferente.

En la analogía, la LSDB funciona como el mapa, y el algoritmo SPF funciona como la persona leyendo el mapa. La LSDB contiene toda la información acerca de todos los posibles routers y enlaces. El algoritmo SPF define cómo un router debe procesar la LSDB, con cada router considerándose a sí mismo como el punto de inicio de la ruta. Cada router se utiliza a sí mismo como el punto de inicio porque cada router necesita insertar rutas en su propia tabla de enrutamiento. El algoritmo SPF calcula todas las posibles rutas para alcanzar una subred, y la métrica acumulativa de cada ruta completa, para cada posible subred de destino. Abreviadamente, cada router debe verse a sí mismo como el punto de inicio, y a cada subred como destino, y utiliza el algoritmo SPF para buscar en el mapa de carreteras LSDB y elegir la mejor ruta a cada subred.

La Figura 8.16 muestra una visión gráfica del resultado del algoritmo SPF ejecutado por el router R1 cuando trata de encontrar la mejor ruta para alcanzar la subred 172.16.3.0/24 (basándose en la Figura 8.15). La Figura 8.16 muestra a R1 en la parte superior de la figura en vez de a la izquierda, porque SPF crea un árbol matemático. Estos árboles normalmente se dibujan con la base o raíz del árbol en la parte superior de la figura, y las hojas (subredes) debajo.

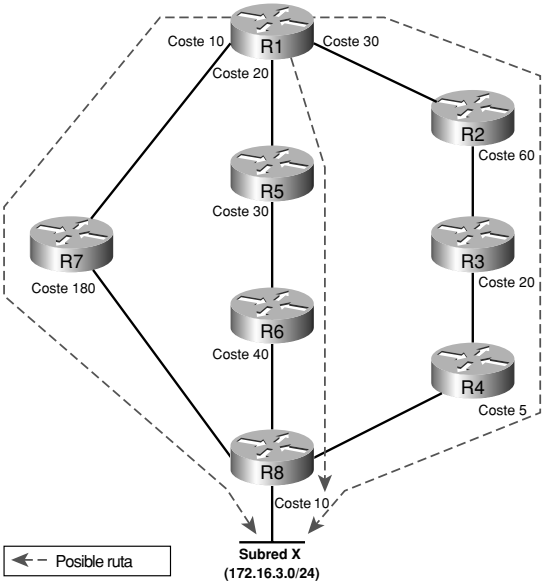


Figura 8.16. Árbol SPF para encontrar la ruta de R1 a 172.16.3.0/24.

La Figura 8.16 no muestra la matemática del algoritmo SPF (francamente, casi nadie se molesta en mirar la matemática), pero muestra un dibujo de la clase de análisis que el algoritmo SPF realiza en R1. Generalmente, cada router ejecuta el proceso SPF para encontrar todas las rutas a cada subred, y entonces el algoritmo SPF puede elegir la mejor ruta. Para elegir la mejor ruta, un algoritmo SPF de un router añade el coste asociado a cada enlace entre sí mismo y la subred de destino, para cada posible ruta. La Figura 8.16 muestra el coste asociado con cada ruta junto a los enlaces; las líneas discontinuas muestran las tres rutas que R1 encuentra entre sí mismo y la subred X (172.16.3.0/24).

La Tabla 8.6 lista las tres rutas mostradas en la Figura 8.16, con sus costes acumulados, mostrando que la mejor ruta de R1 hasta 172.16.3.0/24 empieza por R5.

Tabla 8.6. Comparación de las tres alternaticas de R1 para la ruta hasta 172.16.3.0/24.

Ruta	Lugar en la Figura 8-16	Coste acumulado
R1–R7–R8	Izquierda	10 + 180 + 10 = 200
R1–R5–R6–R8	Centro	20 + 30 + 40 + 10 = 100
R1–R2–R3–R4–R8	Derecha	30 + 60 + 20 + 5 + 10 = 125

Como resultado del análisis del algoritmo SPF de la LSDB, R1 añade una ruta a la subred 172.16.3.0/24 a su tabla de enrutamiento, con R5 como el router de siguiente salto.

Convergencia con los protocolos por estado del enlace

Cuando la internetwork está estable, los protocolos por estado del enlace reinundan cada LSA de forma regular (30 minutos de forma predeterminada para OSPF). Sin embargo, cuando una LSA cambia, los protocolos por estado del enlace reaccionan rápidamente, haciendo converger la red y utilizando las mejores rutas actuales tan rápidamente como sea posible. Por ejemplo, imagine que el enlace entre R5 y R6 falla en la internetwork de las Figuras 8.15 y 8.16. La siguiente lista explica el proceso que R1 utiliza para cambiar a una ruta diferente. (Pasos similares se seguirían para cambios en otros routers y rutas.)

1. R5 y R6 inundan las LSAs que declaran que sus interfaces están ahora en un estado "*down*". (En una red de este tamaño, la inundación normalmente tarda uno o dos segundos.)
2. Todos los routers ejecutan de nuevo el algoritmo SPF para ver si alguna ruta ha cambiado. (Este proceso puede tardar otro segundo en una red de este tamaño.)
3. Todos los routers reemplazan las rutas, si es necesario, basándose en el resultado de SPF. (Esto no tarda prácticamente nada después de que SPF finaliza.) Por ejemplo, R1 cambia su ruta hacia la subred X (172.16.3.0/24) para utilizar R2 como el router de siguiente salto.

Estos pasos permiten al protocolo de enrutamiento por estado del enlace converger rápidamente; mucho más rápidamente que los protocolos de enrutamiento por vector de distancia.

Resumen y comparación con los protocolos por vector de distancia

Los protocolos de enrutamiento por estado del enlace proporcionan una rápida convergencia, que es probablemente la característica más importante de un protocolo de enrutamiento, además de evitar la formación de bucles. Los protocolos de enrutamiento por estado del enlace no necesitan el uso de la gran variedad de características de prevención de bucles utilizadas por los protocolos por vector de distancia, que en sí mismas reducen mucho el tiempo de convergencia. La característica principal de un protocolo de enrutamiento por estado del enlace son las siguientes:

- Todos los routers aprenden la misma información detallada acerca de todos los routers y subredes de la internetwork.
- Las piezas individuales de la información topológica se denominan LSAs. Todas las LSAs se almacenan en RAM en una estructura de datos denominada base de datos de estado del enlace (LSDB).
- Los routers inundan LSAs cuando 1) se crean, 2) en un intervalo de tiempo regular (pero largo) si las LSAs no cambian, y 3) inmediatamente cuando una LSA cambia.

- La LSDB no contiene rutas, pero contiene información que puede ser procesada por el algoritmo SPF de Dijkstra para encontrar la mejor ruta de un router para alcanzar cada subred.
- Cada router ejecuta el algoritmo SPF, con la LSDB como entrada, resultando en que las mejores rutas (menor coste/menor métrica) se añaden a la tabla de enrutamiento IP.

Los protocolos por estado del enlace convergen rápidamente por reinundación inmediata de las LSAs y la reejecución del algoritmo SPF en cada router.

Uno de los puntos de comparación más importante entre los diferentes protocolos de enrutamiento es el tiempo de convergencia. Ciertamente, los protocolos por estado del enlace convergen mucho más rápidamente que los protocolos por vector de distancia. La siguiente lista resume algunos de los puntos clave de comparación para los diferentes protocolos de enrutamiento, comparando los puntos fuertes de los algoritmos subyacentes:

- **Convergencia:** Los protocolos por estado del enlace convergen mucho más rápidamente.
- **CPU y RAM:** Los protocolos por estado del enlace consumen mucha más memoria que los protocolos por vector de distancia, aunque con una planificación apropiada, esta desventaja se puede reducir.
- **Prevención de bucles de enrutamiento:** Los protocolos por estado del enlace inherentemente evitan los bucles, mientras que los protocolos por vector de distancia necesitan de características adicionales (por ejemplo, el horizonte dividido).
- **Esfuerzo de diseño:** Los protocolos por vector de distancia no necesitan de mucha planificación, mientras que los protocolos por estado del enlace requieren de mucha más planificación y esfuerzo de diseño, concretamente en redes grandes.
- **Configuración:** Los protocolos por vector de distancia necesitan normalmente menos configuración, concretamente cuando el protocolo por estado del enlace requiere del uso de características mucho más avanzadas.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, marcados con un icono en el margen exterior de la página. La Tabla 8.7 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 8.7. Temas clave del Capítulo 8.

Tema clave	Descripción	Número de página
Lista	Definiciones y comparación de los términos de protocolo de enrutamiento, protocolo enrutado y protocolo enrutable.	307
Lista	Lista de las funciones principales de un protocolo de enrutamiento.	307
Lista	Definiciones de IGP y EGP.	309
Lista	Tres tipos de algoritmos de enrutamiento IGP.	311
Tabla 8.3	Puntos de comparación de los protocolos IGP.	313
Tabla 8.4	Más comparaciones entre RIP-2, OSPF y EIGRP.	314
Tabla 8.5	Lista de fuentes de información de enrutamiento y sus respectivas distancias administrativas.	315
Figura 8.5	Vista gráfica del significado de vector de distancia.	317
Lista	Descripción de las actualizaciones periódicas del vector de distancia, actualizaciones completas, y actualizaciones completas limitadas por el horizonte dividido.	318
Figura 8.7	Ejemplo de ruta envenenada.	319
Definición	Horizonte dividido.	322
Definiciones	Actualizaciones activadas, inversa envenenada.	324
Definición	*Holddown*.	328
Figura 8.16	Representación gráfica de un cálculo SPF del estado del enlace.	334
Lista	Resumen de las operaciones de estado del enlace.	335-336

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD) o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas ya completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe sus respuestas en el glosario:

Actualización activada, actualización completa, actualización parcial, actualización periódica, algoritmo SPF de Dijkstra, base de datos de estado del enlace (LSDB), convergencia, cuenta hasta infinito, estado del enlace, híbrido equilibrado, *holddown* (temporizador *holddown*), horizonte dividido, infinito, inversa envenenada, métrica, protocolo de enrutamiento, protocolo enrutable, protocolo enrutado, protocolo de gateway exterior (EGP), protocolo de gateway interior (IGP), publicación del estado del enlace (LSA), ruta envenenada, vector de distancia.

Referencias de comandos

Este capítulo no hace referencia a ningún comando que no haya sido tratado de una forma más completa en otro capítulo. Por tanto, este capítulo, al contrario que la mayoría de los otros de este libro, no tiene tablas de referencia de comandos.

Este capítulo trata los siguientes temas:

El protocolo OSPF y su funcionamiento: Esta sección completa nuestra explicación de los protocolos por estado del enlace, que comenzaba en el Capítulo 8, describiendo los detalles del funcionamiento de OSPF.

Configuración de OSPF: Esta sección examina la forma en que se configura OSPF en una sola zona y en varias zonas, la autenticación OSPF y algunas otras características secundarias.

CAPÍTULO 9

OSPF

Los protocolos de enrutamiento por estado del enlace fueron desarrollados en su mayoría en los primeros años de la década de 1990. Los diseñadores de protocolos suponían que las velocidades de los enlaces y de las CPU de los routers, así como sus memorias, irían creciendo con el tiempo. Por tanto, los protocolos se diseñaron para ofrecer unas características mucho más potentes, aprovechando esas mejoras. Al enviar más información y al requerir que los routers efectuasen una mayor cantidad de procesamiento, los protocolos basados en el estado del enlace obtienen ventajas importantes respecto a los protocolos basados en vectores de distancia; en particular, se consigue una convergencia mucho más rápida. El objetivo sigue siendo el mismo, esto es, añadir a la tabla de enrutamiento las mejores rutas de cada instante, pero estos protocolos emplean métodos diferentes para buscar y añadir esas rutas.

Este capítulo explica el protocolo de enrutamiento IP basado en el estado del enlace más extendido: *Open Shortest Path First* (OSPF, Primero la ruta libre más corta). El otro protocolo por estado del enlace para IP, que es IS-IS Integrado, normalmente no se tiene en cuenta en los exámenes de CCNA.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las diez preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 9.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

Tabla 9.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
El protocolo OSPF y su funcionamiento	1-5
Configuración de OSPF	6-10

1. ¿Cuales de las opciones siguientes influyen sobre el cálculo de rutas OSPF cuando se emplean todos los valores predeterminados posibles?
   a. Ancho de banda.
   b. Retardo.
   c. Carga.
   d. Fiabilidad.
   e. MTU.
   f. Número de saltos.
2. OSPF utiliza un algoritmo para calcular la mejor ruta en este instante. ¿Cuáles de los siguientes términos se refieren a ese algoritmo?
   a. SPF.
   b. DUAL.
   c. Sucesor viable.
   d. Dijkstra.
   e. El sentido común.
3. Se conectan dos routers OSPF a la misma VLAN, empleando sus interfaces Fa0/0. ¿Cuáles de los siguientes ajustes de las interfaces de estos dos routers potencialmente vecinos impedirían que se hicieran vecinos OSPF?
   a. Unas direcciones IP de 10.1.1.1/24 y 10.1.1.254/25, respectivamente.
   b. La adición de una dirección IP secundaria en la interfaz de uno de los routers, pero no en el otro.
   c. Asignar a la zona 3 las interfaces de ambos routers.
   d. Un router se configura para utilizar la autenticación MD5 y el otro no se configura para utilizar autenticación.
4. ¿Cuáles de los siguientes estados de vecindad OSPF deberían cambiar cuando finalice el intercambio de información de topología para que los routers vecinos tengan la misma LSDB?
   a. Bidireccional (*Two-way*).
   b. Completa (*Full*).
   c. Intercambio (*Exchange*).
   d. Cargando (*Loading*).
5. ¿Cuáles de las siguientes afirmaciones son verdaderas en lo que respecta a un router OSPF designado y que ya exista?
   a. Si se conecta un nuevo router a la misma subred, y tiene una prioridad OSPF más elevada, se apropiará del DR existente para pasar a ser el nuevo DR.
   b. Si se conecta un nuevo router a la misma subred, y tiene una prioridad OSPF más baja, se apropiará del DR existente para pasar a ser el nuevo DR.
   c. El DR puede ser elegido basándose en el ID de router OSPF más bajo.
   d. El DR puede ser elegido basándose en el ID de router OSPF más alto.

e. El DR intentará pasar a un estado completamente adyacente con todos los demás vecinos de esa subred.

6. ¿Cuáles de los siguientes comandos network, a continuación del comando router ospf 1, indican a este router que empiece a utilizar OSPF en las interfaces cuyas direcciones IP son 10.1.1.1, 10.1.100.1 y 10.1.120.1?

a. network 10.0.0.0 255.0.0.0 area 0

b. network 10.0.0.0 0.255.255.255 area 0

c. network 10.0.0.1 255.0.0.255 area 0

d. network 10.0.0.1 0.255.255.0 area 0

7. ¿Cuáles de los siguientes comandos network, a continuación del comando router ospf 1, indican a este router que empiece a utilizar OSPF en las interfaces cuyas direcciones IP son 10.1.1.1, 10.1.100.1 y 10.1.120.1?

a. network 0.0.0.0 255.255.255.255 area 0

b. network 10.0.0.0 0.255.255.0 area 0

c. network 10.1.1.0 0.x.1x.0 area 0

d. network 10.1.1.0 255.0.0.0 area 0

e. network 10.0.0.0 255.0.0.0 area 0

8. ¿Cuáles de los comandos siguientes producen una lista de los vecinos OSPF que tienen la interfaz serie 0/0?

a. show ip ospf neighbor

b. show ip ospf interface

c. show ip neighbor

d. show ip interface

e. show ip ospf neighbor interface serial 0/0

9. Los routers OSPF R1, R2 y R3 se conectan a una misma VLAN. R2 se ha configurado mediante el subcomando de interfaz ip ospf authentication message-digest en la interfaz LAN que está conectada a la VLAN común. El comando show ip ospf neighbor produce una lista en la que aparecen como vecinos R1 y R3, hallándose éstos en los estados Init y Full, respectivamente. ¿Cuáles de las siguientes afirmaciones son ciertas?

a. R3 debe tener configurado un subcomando de interfaz ip ospf authentication message-digest.

b. R3 debe tener configurado un subcomando de interfaz ip ospf authentication message-digest-key.

c. El fallo de R1 se debe a tener configurado un tipo incorrecto de autenticación OSPF.

d. El fallo de R1 podría o no ser debido a un problema de autenticación.

10. Un router OSPF conoce la existencia de seis rutas posibles para llegar hasta la subred 10.1.1.0/24. Las seis rutas tienen un coste de 55, y las seis son rutas entre

zonas. De manera predeterminada, ¿cuántas de estas rutas se pondrán en la tabla de enrutamiento?

a. 1
b. 2
c. 3
d. 4
e. 5
f. 6

Temas fundamentales

Este capítulo examina los conceptos y la configuración del protocolo OSPF (Primero la ruta libre más corta, *Open Shortest Path First*), y prosigue en el punto en que finalizaba el tratamiento de los estados del enlace en el Capítulo 8. En particular, la primera mitad del capítulo explica toda una gama de temas básicos relacionados con la forma en que funciona OSPF. La segunda parte examina la forma de configurar OSPF en routers Cisco.

El protocolo OSPF y su funcionamiento

El protocolo OSPF posee una amplia gama de posibilidades que, en ocasiones, pueden resultar complejas. Como ayuda para el proceso de aprendizaje, se pueden desglosar las características de OSPF en tres categorías fundamentales: vecinos, intercambio de bases de datos y cálculo de rutas. Los routers OSPF forman en primer lugar una relación de vecindad que sirve como base para todas las comunicaciones OSPF subsiguientes. Una vez que los routers se hacen vecinos, intercambian el contenido de sus respectivas LSDB, mediante un proceso conocido como intercambio de bases de datos. Finalmente, en cuanto un router dispone de información topológica en su base de datos de estado del enlace (LSDB), utiliza el algoritmo de Dijkstra de las rutas más cortas en primer lugar (*Shortest Path First*, SPF) para calcular las que (ahora) son las mejores rutas, y las añade a la tabla de enrutamiento IP.

Es interesante observar que los comandos `show` del IOS también soportan esta misma estructura. El IOS posee una tabla de vecinos OSPF (`show ip ospf neighbor`), una LSDB de OSPF (`show ip ospf database`), y por supuesto una tabla de enrutamiento IP (`show ip route`). Los procesos que se explican en la primera mitad del capítulo se pueden ver en acción en los routers visualizando el contenido de estas tres tablas.

Vecinos en OSPF

Aunque existen ciertas variaciones, la definición general de un vecino OSPF es, desde el punto de vista de un router, otro router que se conecta al mismo enlace de datos con el

que el primer router puede y debe intercambiar información de enrutamiento empleando OSPF. Pese a que esta definición es correcta, se puede comprender mejor el significado real del concepto de vecino en OSPF pensando en el propósito de las relaciones de vecindad en OSPF. En primer lugar, los vecinos comprueban y verifican la configuración básica de OSPF antes de intercambiar información de enrutamiento; estos ajustes tienen que coincidir para que OSPF funcione correctamente. En segundo lugar, el proceso en curso consistente en que un router sabe cuándo el vecino está bien, y cuándo se ha perdido la conexión con el vecino, indica al router el momento en que debe recalcular las entradas de la tabla de enrutamiento para volver a converger en un nuevo conjunto de rutas. Además, el proceso Hello de OSPF define la forma en que se pueden descubrir dinámicamente nuevos vecinos, lo cual significa que se pueden añadir nuevos routers a una red sin que sea preciso reconfigurar todos y cada uno de los routers.

El proceso Hello de OSPF mediante el cual se forman nuevas relaciones de vecindad se parece en cierto modo a trasladarse a otra casa, y conocer a nuestros nuevos vecinos. Cuando se encuentra uno con un vecino fuera de casa, nos acercamos y nos saludamos, y nos decimos nuestros nombres. Después de hablar un rato, uno se forma una primera impresión, y en particular uno sabe si le gustará hablar un ratito de vez en cuando con ese vecino, o si la próxima vez que nos encontremos le diremos adiós y no nos detendremos para charlar. De manera similar, en OSPF el proceso comienza con unos mensajes llamados Hello. Los Hello indican el ID de router (RID) de los routers, que hace las veces de nombre exclusivo del router o como identificador para OSPF. Finalmente, OSPF hace varias comprobaciones de la información que hay en los mensajes Hello para asegurarse de que ambos routers deben hacerse vecinos.

Identificación de routers OSPF mediante un ID de router

OSPF necesita identificar de forma exclusiva a todos los routers por muchas razones. En primer lugar, los vecinos necesitan disponer de una forma de saber qué router ha enviado un cierto mensaje de OSPF. Además, la LSDB de OSPF contiene un conjunto de Publicaciones de estado del enlace (*Link State Advertisements*, LSA), algunas de las cuales describen a todos los routers de la red, así que la LSDB necesita un identificador exclusivo para cada router. Con este fin, OSPF utiliza un concepto denominado **ID de router** (RID) de OSPF.

Los RID de OSPF son números de 32 bits escritos en decimal con puntos, así que el uso de una dirección IP es una forma cómoda de buscar un RID predeterminado. Alternativamente, el RID de OSPF se puede configurar de forma directa, según se describe en una sección posterior denominada "Configuración del ID de router en OSPF."

Búsqueda de vecinos diciendo Hello

En cuanto el router ha seleccionado su RID OSPF, y se activan unas cuantas interfaces, el router queda preparado para encontrarse con sus vecinos OSPF. Los routers OSPF pueden hacerse vecinos si están conectados a la misma subred (y en algunos otros casos especiales que no se tratan en los exámenes CCNA). Para descubrir a otros routers que se

comuniquen mediante OSPF, el router envía paquetes Hello de OSPF por multidifusión a todas las interfaces, con la esperanza de recibir paquetes Hello de otros routers que estén conectados a esas interfaces. La Figura 9.1 esboza el concepto básico.

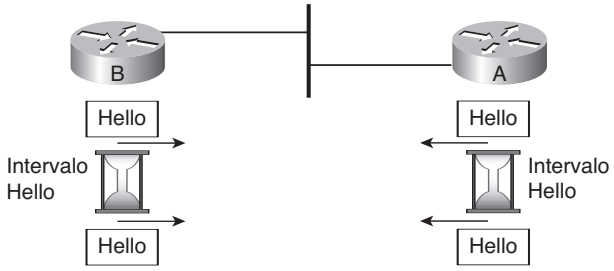


Figura 9.1. Paquetes Hello de estado del enlace.

Tanto el router A como el B envían mensajes Hello a través de la LAN. Siguen enviando mensajes Hello basándose en la configuración del temporizador Hello. Poco después, los dos routers pueden empezar a intercambiar información topológica entre sí. Entonces podrán emplear el algoritmo de Dijkstra para rellenar la tabla de enrutamiento con las mejores rutas. Los mensajes Hello en sí poseen las características siguientes:

- El mensaje Hello sigue al encabezado del paquete IP, y tiene un tipo de protocolo de paquete IP de valor 89.
- Los paquetes Hello se envían a la dirección IP de multidifusión 224.0.0.5, que es una dirección IP de multidifusión destinada a todos los routers que se comunican mediante OSPF.
- Los routers OSPF quedan a la escucha de paquetes enviados a la dirección IP de multidifusión 224.0.0.5, esperando en parte recibir paquetes Hello y aprender sobre nuevos vecinos.

Los routers aprenden varios elementos de información importantes mediante el examen de los paquetes Hello que reciben. El mensaje Hello incluye el RID del router remitente, el ID de zona, el intervalo de Hello, el intervalo muerto, la prioridad del router, el RID del router designado, el RID del router designado de respaldo, y una lista de vecinos que el router remitente ya conoce en la subred. (En el futuro se ofrecerá más información sobre casi todas estas informaciones.)

La lista de vecinos tiene especial importancia para el proceso Hello. Por ejemplo, cuando el Router A recibe un Hello procedente del Router B, el Router A necesita indicar de algún modo al Router B que el Router A ha recibido el Hello. Para hacer esto, el Router A añade el RID del Router B a la lista de vecinos OSPF que hay en el próximo Hello (y en los subsiguientes) que el Router A enviará a la red por multidifusión. De manera análoga, cuando el Router B reciba el Hello del Router A, el próximo Hello del Router B (y los subsiguientes) incluirán el RID del Router A en la lista de vecinos.

En cuanto un router observa su propio RID en un Hello que ha recibido, el router piensa que se ha establecido una comunicación **bidireccional** con ese vecino. El estado bidirec-

cional (o de dos vías) de un vecino es importante, porque en ese momento se puede intercambiar información más detallada, como las LSAs. Además, en ciertos tipos de LAN, los vecinos pueden llegar al estado bidireccional y quedarse así. Se ofrecerá más información sobre esta cuestión en la sección "Selección de un router designado".

Problemas potenciales para llegar a hacerse vecinos

Curiosamente, recibir un Hello de un router de la misma subred no siempre da lugar a que dos routers se hagan vecinos. Es como conocer a un vecino nuevo en la vida real. Si los vecinos discrepan respecto a muchas cosas, y no se llevan bien entre sí, posiblemente no lleguen a hablar mucho. De forma similar, en OSPF, los routers de una misma subred tienen que estar de acuerdo respecto a varios de los parámetros que se intercambian en el Hello; en caso contrario, los routers simplemente no llegarán a ser vecinos. Específicamente, tiene que coincidir lo siguiente para que dos routers se hagan vecinos:

- La máscara de subred empleada en la subred.
- El número de subred (que se obtiene empleando la máscara de subred y la dirección IP de la interfaz de cada uno de los routers).
- El intervalo de Hello.
- El intervalo muerto.
- El ID de área OSPF.
- Tienen que pasar las comprobaciones de autenticación (si se usan).
- Valor del indicador de área interna (*stub area*).

Si difiere alguno de estos parámetros, los routers no se hacen vecinos. En resumen, si se están resolviendo problemas de OSPF relacionados con que ciertos routers deberían hacerse vecinos, y no lo hacen, entonces ¡hay que comprobar esta lista!

Nota

El indicador de área interna (*stub area*) está relacionado con conceptos que van más allá de los límites de los exámenes CCNA, pero se incluye aquí como requisito para que dos routers se hagan vecinos únicamente para que la lista quede completa.

Hay un par de elementos de la lista que requieren una explicación adicional. En primer lugar, los vecinos potenciales confirman que se hallan en la misma subred comparando la dirección IP y la máscara de subred de los routers, según se indica en el mensaje Hello, con su propia dirección y máscara. Si se encuentran exactamente en la misma subred, con el mismo rango de direcciones, entonces esta comprobación se da por válida.

Además, tienen que coincidir dos ajustes de temporizadores, el intervalo de Hello y el intervalo muerto. Los routers OSPF envían mensajes Hello a intervalos marcados por el intervalo de Hello. Cuando un router no recibe un Hello de un vecino durante el tiempo estipulado por el intervalo muerto, el router piensa que el vecino ya no está disponible, y reacciona haciendo que vuelva a converger la red. Por ejemplo, en interfaces Ethernet, los routers de Cisco tienen un intervalo de Hello predefinido de 10 segundos, y un intervalo muerto de

4 veces el intervalo de Hello, que son 40 segundos. Si un router no recibe ningún mensaje Hello de un vecino durante 40 segundos, marca ese router (que no responde en estos momentos) como "*down*" en su tabla de vecinos. En ese momento, los routers pueden reaccionar y converger para utilizar las rutas que sean realmente óptimas en este instante.

Estados de vecindad

OSPF define un extenso conjunto de acciones potenciales que pueden utilizar dos vecinos para comunicarse entre sí. Para hacer un seguimiento del proceso, los routers OSPF atribuyen a cada vecino un estado de entre los muchos que puede tener un vecino en OSPF. El estado de vecindad en OSPF es la percepción que tiene el router de la cantidad de trabajo que ya se ha realizado en los procesos normales llevados a cabo por dos routers vecinos. Por ejemplo, si los routers R1 y R2 se conectan a la misma LAN y se hacen vecinos, R1 atribuye un estado de vecindad para R2, que es la percepción que tiene R1 respecto a lo que ha sucedido entre R2 y R1 hasta el momento. (El comando más frecuente para enumerar los vecinos y sus estados es `show ip ospf neighbor`.)

Como los estados de vecindad reflejan varios aspectos de los procesos OSPF que se utilizan normalmente entre dos routers, resulta útil discutir los estados de vecindad junto con estos procesos y con los mensajes de OSPF. Además, al comprender los estados OSPF y sus significados, los ingenieros pueden determinar con mayor facilidad si un vecino OSPF funciona normalmente, o si hay algún problema.

La Figura 9.2 muestra varios estados que se utilizan al comienzo de la formación de una relación de vecindad. La Figura muestra los mensajes Hello y los estados de vecindad resultantes.

Figura 9.2. Estados iniciales de vecindad.

Los dos primeros estados, que son los estados *Down* (inactivo) e *Init* (arrancando) son relativamente sencillos. En aquellos casos en que un router ya conocía la existencia de un vecino, pero ha fallado la interfaz, el vecino se pone en la lista con el estado *Down*. En cuanto se activa la interfaz, los dos routers pueden enviar mensajes Hello, dando lugar a que ese vecino pase a un estado *Init*. Este estado significa que la relación de vecindad se está inicializando.

Los routers pasan del estado *Init* a un estado bidireccional cuando se dan dos circunstancias importantes: hay un Hello recibido que contiene en su lista el RID del router como visto (*seen*), y ese router ha comprobado todos los parámetros del vecino y le parecen correctos. Estos dos hechos denotan que el router está dispuesto a comunicarse con su vecino. Para que funcione el proceso, cuando cada router recibe un Hello de un nuevo vecino, el router comprueba los detalles de configuración del nuevo vecino, según se ha descrito anteriormente. Si todo parece estar bien, el próximo Hello del router contiene el RID del vecino en la lista de routers vistos ("*seen*"). Una vez que ambos routers han comprobado los parámetros y han enviado un listado Hello en el que aparece el RID del otro como visto, ambos routers han alcanzado el estado bidireccional.

Por ejemplo, en la Figura 9.2, R2 recibe el primer Hello, que muestra "Seen [null]". Esta notación significa que R1 todavía no ha visto ningún vecino potencial. Cuando R2 envía su Hello, R2 muestra el RID de R1, implicando que R2 ha visto a R1 y ha verificado que todos los parámetros le parecen bien. R1 devuelve el favor en el tercer Hello, que se envía un intervalo Hello después del primer Hello de R1.

Una vez que se encuentran en un estado bidireccional, los dos routers están dispuestos para intercambiar información sobre su topología, según se describe en la sección siguiente.

Intercambio de la base de datos topológica de OSPF

Los routers OSPF intercambian el contenido de sus LSDB para que ambos vecinos tengan una copia exacta de la misma LSDB al finalizar el proceso de intercambio de bases de datos; esto es un principio fundamental de la forma en que operan los protocolos de enrutamiento basados en el estado del enlace. El proceso tiene muchos pasos, y tiene muchos más detalles que los que se cuentan aquí. Esta sección comienza por explicar una visión general de todo el proceso, y va seguida por un examen más detallado de cada paso.

Visión general del proceso de intercambio de bases de datos de OSPF

Curiosamente, una vez que dos routers OSPF se hacen vecinos y alcanzan un estado bidireccional, el paso siguiente puede no ser el intercambio de información topológica. En primer lugar, basándose en varios factores, los routers tienen que decidir si deben intercambiar información topológica directamente, o si los dos vecinos deben aprender la información topológica del otro indirectamente, en forma de LSA. En cuanto una pareja de vecinos OSPF sabe que deberían compartir información topológica directamente, intercambian los datos de topología (las LSAs). Una vez hecho esto, el proceso pasa a un estado de mantenimiento relativamente tranquilo en el que los routers vuelven a rellenar ocasionalmente las LSAs y vigilan en busca de cambios en la red.

El proceso general se desarrolla en la forma siguiente; cada paso se explica en las páginas siguientes:

Paso 1 Basándose en el tipo de interfaz OSPF, los routers pueden elegir colectivamente (o no) un Router designado (DR) y un Router designado de respaldo (BDR).

Paso 2 Para cada pareja de routers que necesitan pasar a ser completamente adyacentes, se efectúa un intercambio mutuo de sus respectivas LSDB.

Paso 3 Cuando han terminado, los vecinos vigilan en busca de cambios y vuelven a rellenar periódicamente las LSAs mientras se encuentren en el estado de vecindad *Full* (completamente adyacente).

Selección de un router designado

OSPF exige que las subredes o bien usen o bien no usen un Router designado (DR) y un Router designado de respaldo (BDR) basándose en el tipo de interfaz OSPF (que a veces se denomina también tipo de red OSPF). Existen varios tipos de interfaces OSPF, pero para los exámenes de CCNA hay que conocer dos tipos principales: punto a punto y de difusión. (Estos tipos se pueden configurar empleando el comando `ip ospf network` *tipo*.) Estos tipos de interfaz OSPF son una referencia general del tipo de protocolo de enlace de datos utilizado. Como puede suponerse a partir de los nombres, el tipo punto a punto sirve para enlaces punto a punto, y el tipo difusión sirve para utilizarlo en enlaces de datos que admitan tramas de difusión, como las LANs.

La Figura 9.3 muestra un ejemplo clásico de dos conjuntos de vecinos: uno que utiliza el tipo de interfaz OSPF predeterminado de punto a punto en un enlace serie, y otro que utiliza el tipo de interfaz predeterminado OSPF de difusión en una LAN. El resultado final de la elección de DR es que sólo se intercambia información topológica entre los vecinos que se muestran unidos por líneas con flechas en la figura. Observe la parte inferior derecha de la figura.

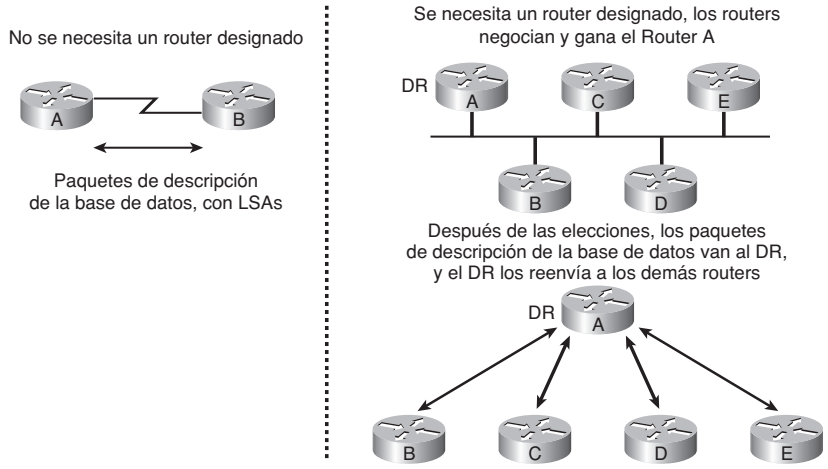


Figura 9.3 Sin DR en un enlace punto a punto, con un DR en la LAN.

Cuando no se requiere un DR, los routers vecinos pueden proseguir y comenzar el proceso de intercambio de topología, según se muestra en el lado izquierdo de la figura. En la terminología de OSPF, los dos routers de la izquierda deberían seguir trabajando para intercambiar información topológica y llegar a ser totalmente adyacentes. En el lado derecho de la figura, la parte superior muestra una topología de LAN en la que se ha celebrado una elección de DR, y el Router A ha ganado las elecciones. Con un DR, el proceso de intercambio de topología se produce entre el DR y todos los demás routers, pero no entre todas las parejas de routers. En consecuencia, todas las actualizaciones de enrutamiento fluyen desde y hacia el Router A, y en esencia el Router A distribuye la información topológica a los demás routers. Todos los routers aprenden toda la información topológica de todos los otros routers, pero el proceso sólo da lugar a intercambio directo de información entre el DR y cada uno de los routers que no son el DR.

El concepto de DR evita sobrecargar las subredes con un tráfico excesivo de OSPF cuando hay muchos routers en una subred. Por supuesto, se podrían conectar muchos routers a una LAN, razón por la cual se requiere un DR para los routers conectados a una LAN. Por ejemplo, si se conectasen diez routers a la misma subred de una LAN, y se les permitiese reenviar actualizaciones de OSPF a cada uno de los otros nueve routers, entonces se pasarían actualizaciones de topología entre 45 parejas distintas de vecinos, ¡y casi toda la información sería redundante! Mediante el concepto de DR, según se muestra en el lado derecho de la Figura 9.3, esa misma LAN requeriría actualizaciones sólo entre el DR y los otros nueve routers, reduciendo significativamente la avalancha de información OSPF a través de la LAN.

Como el DR es tan importante para el intercambio de información de enrutamiento, la pérdida del DR seleccionado puede causar retardos en la convergencia. OSPF posee también el concepto de **Router de respaldo** (*backup router*, BDR) en todas las subredes, de tal modo que si falla el DR o pierde conectividad con la subred, el BDR puede hacer las veces de DR. (Todos los routers salvo el DR y el BDR se denominan normalmente "DROther" en el resultado del comando show del IOS.)

Nota

Todos los routers que no son DR ni BDR intentan hacerse completamente adyacentes tanto con el DR como con el BDR, pero la Figura 9.3 muestra solamente las relaciones existentes con el DR para reducir la complejidad de la imagen.

Cuando se requiere un DR, los routers vecinos celebran unas elecciones. Para elegir un DR, los routers vecinos examinan dos campos que hay dentro de los paquetes Hello que reciben, y eligen al DR basándose en los criterios siguientes:

- El router que envía el Hello con el valor de **prioridad OSPF más alto** pasa a ser el DR.
- Si dos o más routers empatan por tener el valor de prioridad más elevado, el router que envíe el **RID más alto** será el ganador.
- No siempre sucede, pero normalmente el router que tiene la segunda prioridad más alta es el que pasa a ser el BDR.

- Un ajuste de prioridad igual a 0 significa que ese router no participará en las elecciones, y por tanto nunca puede llegar a ser DR o BDR.
- El rango de valores de prioridad que permiten que un router sea candidato va desde 1 hasta 255.
- Si aparece un candidato nuevo y mejor después de que se hayan elegido el DR y el BDR, el nuevo candidato no intenta desplazar al DR y al BDR existentes.

Intercambio de bases de datos

El proceso de intercambio de bases de datos puede ser bastante complejo, con distintos mensajes OSPF. Se pueden ignorar los detalles del proceso para los propósitos de este libro, pero una pequeña visión general puede servir de ayuda para adquirir cierta perspectiva del proceso general.

Una vez que dos routers deciden intercambiar sus bases de datos, no se limitan a enviar el contenido de toda la base de datos. En primer lugar, se dicen uno a otro la lista de LSAs que hay en sus respectivas bases de datos, pero no todos los detalles de las LSAs, sólo una lista. Después cada router compara la lista del otro router con su propia LSDB. De aquellas LSAs de las que el router no tenga una copia, pedirá al router vecino una copia de esa LSA, y entonces el router vecino le enviará la LSA completa.

Cuando dos vecinos han terminado este proceso, se considera que han terminado por completo el proceso de intercambio de bases de datos. Por tanto, OSPF emplea el estado de vecindad *Full* (completo) para denotar que el proceso de intercambio de la base de datos se ha completado.

Mantenimiento de la LSDB cuando el router es completamente adyacente

Los vecinos que se encuentran en estado *Full* siguen realizando ciertas tareas de mantenimiento. Siguen enviando mensajes Hello a cada intervalo de Hello. La ausencia de mensajes Hello durante un tiempo igual al intervalo muerto significa que la conexión con el vecino ha fallado. Además, si se produce algún cambio de topología, los vecinos enviarán nuevas copias de las LSAs modificadas a cada vecino, para que el vecino pueda cambiar sus LSDBs. Por ejemplo, si falla una subred, el router actualiza la LSA de esa subred, con objeto de reflejar que esa subred ha fallado. Entonces el router envía la LSA a sus vecinos, y éstos a su vez la envían a los suyos, hasta que todos los routers tengan de nuevo una copia idéntica de una misma LSDB. Entonces los routers pueden utilizar también el SPF para recalcular las rutas que puedan haber resultado afectadas por la subred que ha fallado.

El router que crea cada LSA tiene también la responsabilidad de reinundar la LSA cada 30 minutos (de forma predeterminada), aun cuando no se hayan producido cambios. Este proceso es bastante distinto del concepto de actualizaciones periódicas propio de los vectores de distancia. Los protocolos por vector de distancia envían actualizaciones comple-

tas en un breve periodo de tiempo, y enumeran en ellas todas las rutas (salvo las que se omiten debido a herramientas para evitar bucles, como el horizonte dividido). OSPF no envía todas las rutas cada 30 minutos. En lugar de hacer esto, cada LSA tiene un temporizador propio, basado en el momento en que se ha creado la LSA. Por tanto, no hay un único momento en que OSPF envíe un montón de mensajes para reinundar las LSAs. En lugar de hacer esto, las LSAs son reinundadas por parte del router que ha creado la LSA, cada 30 minutos.

Como recordatorio, hay algunos routers que no intentan llegar a ser completamente adyacentes. En particular, en aquellas interfaces en las que se ha elegido un DR, los routers que no son DR ni BDR se hacen vecinos, pero no se hacen completamente adyacentes. Estos routers que no son completamente adyacentes no intercambian sus LSAs de forma directa. Además, el comando `show ip ospf neighbor` ejecutado en uno de estos routers pone a estos vecinos en la lista como dotados de un estado bidireccional como estado normal estable del vecino, y establece para el DR y el BDR el estado normal estable *Full*.

Resumen de los estados de los vecinos

Para facilitar la referencia y el estudio, la Tabla 9.2 enumera y describe brevemente los estados de vecindad mencionados en este capítulo.

Tabla 9.2. Estados de vecindad de OSPF y sus significados.

Estado del vecino	Significado
Down	Un vecino conocido no está disponible, frecuentemente debido a un fallo de la interfaz subyacente.
Init	Un estado intermedio en el que se ha escuchado un Hello procedente del vecino, pero en ese Hello no se muestra el RID del router como visto anteriormente.
Two-way (bidireccional)	El vecino ha enviado un Hello que muestra el RID del router local en la lista de routers vistos, lo cual implica también que todas las comprobaciones de verificación del vecino se han completado con éxito.
Full	Los dos routers conocen exactamente los mismos detalles de la LSDB y son completamente adyacentes.

Construcción de la tabla de enrutamiento IP

Los routers OSPF envían mensajes para aprender sobre sus vecinos, mostrando estos vecinos en la tabla de vecinos de OSPF. Después, los routers OSPF envían mensajes para intercambiar datos topológicos con esos mismos vecinos, almacenando la información en la tabla de topología de OSPF, que suele llamarse LSDB o base de datos de OSPF. Para

rellenar la tercera tabla importante que utiliza OSPF, y que es la tabla de enrutamiento IP, OSPF no envía mensaje alguno. Cada router ejecuta el algoritmo SPF de Dijkstra aplicado a la base de datos topológica de OSPF, y selecciona las mejores rutas basándose en ese proceso.

La base de datos topológica de OSPF está formada por listas de números de subredes (que se denominan *enlaces*, razón por la cual se habla de una **base de datos de estado del enlace**). También contiene listas de routers, junto con los enlaces (las subredes) a las que está conectado cada router. Disponiendo del conocimiento de los enlaces y de los routers, un router puede ejecutar el algoritmo SPF para calcular las mejores rutas de acceso a todas las subredes. El concepto se parece bastante al de hacer un *puzzle* o rompecabezas. El color y la forma de las piezas sirven de ayuda para identificar las piezas que pueden encajar con una pieza dada. De forma similar, la información detallada que hay en cada LSA (datos tales como una LSA de enlaces que enumera los routers conectados a la subred, y una LSA de routers que enumera sus direcciones IP y sus máscaras) dan al algoritmo SPF información suficiente para calcular qué routers están conectados a cada subred y para crear el equivalente matemático de un diagrama de la red.

Cada router utiliza independientemente el algoritmo SPF de Dijkstra, aplicándolo a la LSDB de OSPF con objeto de hallar la mejor ruta que va desde ese router hasta cada una de las subredes de la LSDB. Entonces el router pone la mejor ruta hasta cada subred en la tabla de enrutamiento IP. Parece sencillo, y lo es si se dispone de un dibujo de la red que aporte toda la información. Afortunadamente, aun cuando las matemáticas subyacentes al algoritmo SPF pueden resultar intimidantes, no es preciso conocer las matemáticas de SPF para los exámenes, ni tampoco para desempeñar trabajos en el mundo de las redes reales. Sin embargo, sí es preciso ser capaz de predecir las rutas que seleccionará SPF empleando diagramas de red y la documentación.

OSPF selecciona la ruta de coste mínimo para acceder desde el router hasta la subred. Esto se hace sumando los costes OSPF de las interfaces salientes. Cada interfaz tiene asociado un coste OSPF. El router examina todas las posibles rutas, suma los costes de las interfaces por las cuales se enviarían paquetes a esa ruta, y después selecciona la ruta de coste mínimo. Por ejemplo, la Figura 9.4 muestra una red sencilla en la que se especifica el coste OSPF junto a cada interfaz. En esta figura, el router R4 posee dos posibles rutas mediante las cuales puede acceder a la subred 10.1.5.0/24. Las dos rutas son las siguientes, donde aparece cada router y su interfaz saliente:

R4 Fa0/0—R1 S0/1—R5 Fa0/0
R4 Fa0/0—R2 S0/1—R5 Fa0/0

Si se suman los costes asociados a cada interfaz, la primera de las dos rutas tiene un coste total de 111, y la segunda tiene un coste total de 75. Por tanto, R4 añade la ruta que pasa por R1 como mejor ruta, y muestra la dirección IP de R1 como dirección IP del siguiente salto.

Ahora que ya se ha visto la forma en que los routers OSPF llevan a cabo las funciones más fundamentales de OSPF, la sección siguiente examina OSPF de forma más general, y estudia especialmente algunas consideraciones importantes sobre el diseño.

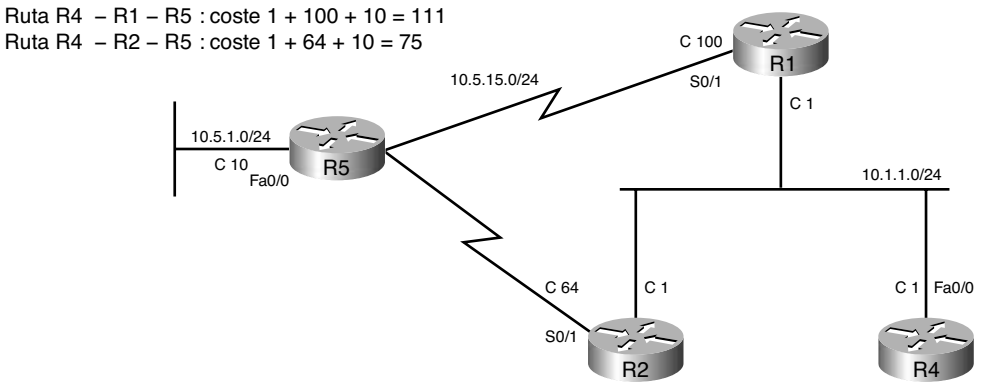


Figura 9.4. Ejemplo de red OSPF mostrando los costes.

Escalado de OSPF mediante un diseño jerárquico

OSPF se puede utilizar en ciertas redes sin pensar mucho en cuestiones de diseño. Basta activar OSPF en todos los routers, y todo funciona. Sin embargo, en redes grandes los ingenieros tienen que pensar y deben planear la forma de emplear varias características de OSPF que hacen posible que crezca correctamente en redes aún más grandes. Para apreciar los problemas que subyacen a la escalabilidad de OSPF, y la necesidad de un buen diseño para hacer posible la escalabilidad, considere la Figura 9.5.

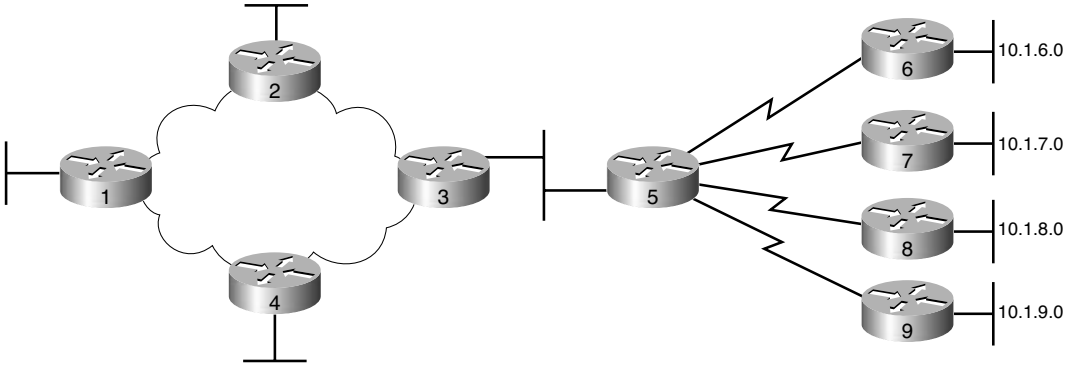


Figura 9.5. OSPF de una sola área.

En la red que se muestra en la Figura 9.5, la base de datos topológica de los nueve routers es la misma topología completa que sugiere la figura. En una red de este tamaño, puede uno limitarse a activar OSPF y funcionará perfectamente. Pero imagine una red con 900 routers en lugar de sólo nueve, y varios miles de subredes. En una red de semejante tamaño, la mera cantidad de procesamiento necesaria para ejecutar el complejo algoritmo SPF

podría dar lugar a unos tiempos de convergencia muy elevados, y los routers podrían sufrir problemas por agotamiento de su memoria. Los problemas se pueden resumir de la siguiente forma:

Tema clave

- Una base de datos de topología más grande requiere más memoria en todos los routers.
- El procesamiento de una base de datos para una topología más extensa mediante el algoritmo SPF requiere una potencia de procesamiento que crece exponencialmente con el tamaño de la base de datos topológica.
- ¡Un solo cambio de estado en una interfaz (de activa a inactiva o de inactiva a activa) obligará a todos los routers a ejecutar de nuevo el SPF!

Aunque en este contexto no existe una definición exacta de "grande", en aquellas redes que tengan al menos 50 routers y al menos unos pocos cientos de subredes, los ingenieros deben utilizar las características de escalabilidad de OSPF para reducir los problemas descritos. Estos números son simplemente generalizaciones. Dependen sobre todo del diseño de la red, de la potencia de la CPU del router, de la cantidad de RAM de que disponga, etc.

Áreas de OSPF

El uso de áreas OSPF resuelve muchos de los problemas comunes que aparecen al ejecutar OSPF en grandes redes, pero no todos. Las áreas OSPF fragmentan la red de tal modo que los routers de cada área tienen menos información topológica sobre las subredes presentes en otras áreas; además, desconocen por completo la existencia de los routers de las otras áreas. Al utilizar unas bases de datos topológicas más reducidas, los routers consumen menos memoria y requieren menos tiempo de procesamiento para ejecutar el algoritmo SPF. La Figura 9.6 muestra la misma red que la Figura 9.5, pero con dos áreas OSPF, que se han rotulado como Área 1 y Área 0.

En la parte superior de la figura se muestra la misma topología, pero en la parte inferior de la figura se muestra la base de datos topológica de los Routers 1, 2 y 4. Al situar parte de la red en otra área, los routers que se encuentran dentro de Área 1 quedan protegidos de algunos de los detalles. El Router 3 se conoce con el nombre de Router fronterizo (*Area Border Router*, ABR) OSPF, porque se encuentra en la frontera que media entre dos áreas distintas. El Router 3 no publica la información topológica completa relativa al área de la red que se encuentra en Área 0 a los Routers 1, 2 y 4. En lugar de hacer esto, el Router 3 publica una información resumida relativa a las subredes de Área 0, y a todos los efectos hace que los Routers 1, 2 y 4 piensen que la topología tiene el aspecto que se muestra en la parte inferior de la Figura 9.6. Por tanto, los Routers 1, 2 y 4 ven el mundo como si tuviese menos routers. Como resultado, el algoritmo SPF requiere menos tiempo y la base de datos topológica ocupa menos memoria.

El diseño de OSPF introduce unos pocos términos importantes que es preciso conocer para los exámenes; se han definido en la Tabla 9.3.

Es muy importante apreciar la diferencia que existe entre la información resumida que se muestra en la Figura 9.6 y las rutas resumidas que se tratan en el Capítulo 5. En este caso, el término "resumen" sólo indica que un router situado dentro de un área recibe una

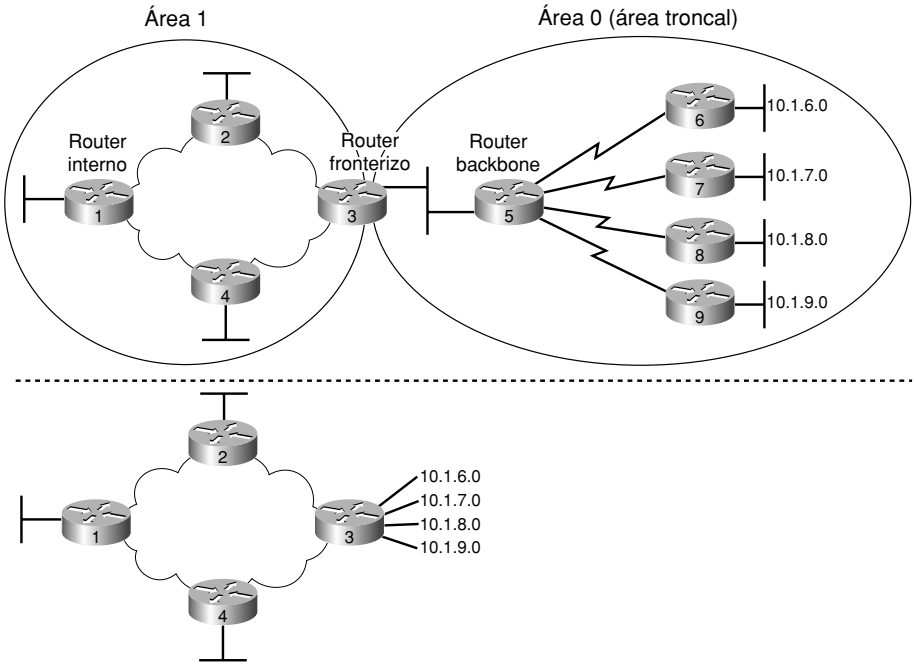


Figura 9.6. OSPF de dos áreas.

Tabla 9.3. Terminología de diseño para OSPF.

Término	Significado
Router fronterizo (ABR)	Es un router OSPF que tiene interfaces conectadas al área backbone y al menos a otra área más.
Router fronterizo de sistema autónomo (ASBR)	Es un router OSPF que se conecta con routers que no hacen uso de OSPF con el propósito de intercambiar rutas externas que entren y salgan del dominio OSPF.
Router backbone	Un router situado en un área, el área backbone.
Router interno	Un router situado en una sola área no backbone.
Área	Un conjunto de routers y enlaces que comparten la misma información detallada en la LSDB, pero sin routers en otras áreas, para mayor eficiencia.
Área backbone (troncal)	Un área OSPF especial a la que deben conectarse todas las demás áreas. Área 0.
Ruta externa	Una ruta conocida aunque no está dentro del dominio OSPF y que después se publica en el dominio OSPF.
Ruta intra-área	Una ruta que lleva a una subred de la misma área que el router.
Ruta interárea	Ruta que lleva a una subred de un área en la que no se encuentra el router.
Sistema autónomo	En OSPF, denota un conjunto de routers que emplean OSPF.

información más breve en la LSA de una subred, y por tanto se reduce la cantidad de memoria necesaria para almacenar la información. Por ejemplo, en la Figura 9.6, el router R1 (que está en Área 1) sólo llega a conocer una LSA muy breve respecto a las subredes que están en Área 0. Este proceso reduce el tamaño y complejidad del algoritmo SPF. Además, el término "resumen" puede hacer alusión a una ruta resumida que se configure en OSPF, con los conceptos generales que se tratan en el Capítulo 5. El resumen manual de rutas OSPF reduce el número de subredes, lo cual a su vez reduce también el tamaño y esfuerzo necesarios para el cálculo SPF.

Nota

Aunque las perspectivas de los routers que están en Área 1 se muestran en la Figura 9.6, sucede lo mismo en el sentido inverso; los routers de Área 0 no conocen los detalles de la topología de Área 1.

Obsérvese que la línea divisoria entre áreas no es un enlace, sino un router. En la Figura 9.6, el Router 3 se encuentra tanto en Área 1 como en Área 0. OSPF utiliza el término Router fronterizo (*Area Border Router*, ABR) para describir aquellos routers que se hallan en ambas áreas. Los ABRs contienen la base de datos topológica de ambas áreas, y ejecutan el algoritmo SPF cuando cambian los enlaces en cualquiera de las áreas. Por tanto, aunque el uso de áreas ayuda al crecimiento de OSPF por reducir el tamaño de la LSDB y el tiempo necesario para calcular las tablas de enrutamiento, la cantidad de RAM y de CPU que consumen los ABRs puede llegar a crecer. Como resultado, los routers que actúen como ABR deberán ser routers más rápidos y disponer de una cantidad de memoria comparativamente mayor.

Ventajas que aportan las áreas en el diseño de OSPF

El uso de áreas mejora las operaciones de OSPF en muchos sentidos, especialmente en las redes más extensas:

- Al ser más pequeña la LDSB de cada área, se requiere menos memoria.
- El router necesita menos ciclos de CPU para procesar la LDSB de cada área mediante el algoritmo SPF; esto reduce el gasto de CPU y mejora el tiempo de convergencia.
- El algoritmo SPF sólo tiene que ejecutarse en routers interiores cuando cambia una LSA situada dentro del área, así que los routers ejecutan el SPF con menos frecuencia.
- Es preciso intercambiar menos información entre áreas, lo cual reduce el ancho de banda necesario para enviar las LSAs.
- El resumen manual sólo se puede configurar en los ABRs y ASBRs, así que las zonas dan lugar a tablas de enrutamiento IP más pequeñas, puesto que permiten la configuración manual de resúmenes de rutas.

Configuración de OSPF

La configuración de OSPF sólo tiene unos pocos pasos obligatorios, pero tiene muchos pasos opcionales. Una vez seleccionado el diseño OSPF (y esta tarea puede ser compleja en las redes IP más extensas) la configuración puede ser tan sencilla como habilitar OSPF en la interfaz de todos los routers y poner esa interfaz en el área correcta de OSPF.

Esta sección muestra varios ejemplos de configuración, comenzando por una red OSPF de una sola área y pasando después a una red OSPF con múltiples áreas. Después de estos ejemplos, el texto pasa a tratar varios de los ajustes de configuración opcional adicionales. Como referencia, la lista siguiente esboza los pasos de configuración que se tratan en este capítulo, y también muestra una breve referencia de los comandos obligatorios:

Paso 1 Entrar en el modo de configuración OSPF de un determinado proceso OSPF, empleando el comando global router ospf *id-proceso*.

Paso 2 (Opcional) Configurar el ID del router OSPF haciendo lo siguiente:

- Configurar el subcomando router-id *valor-id* del router.
- Configurar una dirección IP en una interfaz *loopback*.

Paso 3 Configurar uno o más subcomandos network *dirección-ip máscara-wildcard* area *id-área* del router, añadiéndose las interfaces coincidentes al área enumerada.

Paso 4 (Opcional) Modificar los intervalos Hello y muerto de la interfaz, empleando los subcomandos ip ospf hello-interval *tiempo* e ip ospf dead-interval *tiempo*.

Paso 5 (Opcional) Influir sobre las opciones de enrutamiento haciendo lo siguiente:

- Configurar directamente los costes mediante el subcomando de interfaz ip ospf cost *valor*.
- Modificar los anchos de banda de la interfaz utilizando el subcomando bandwidth *valor*.

c. Cambiar el numerador de la fórmula para calcular el coste basado en el ancho de banda de la interfaz, utilizando el subcomando de router auto-cost reference-bandwidth *valor*.

Paso 6 (Opcional) Configurar la autenticación de OSPF:

- Interfaz por interfaz, empleando el subcomando de interfaz ip ospf authentication.
- Para todas las interfaces de un área, empleando el subcomando de router area authentication.

Paso 7 (Opcional) Configurar el soporte para múltiples rutas de igual coste, empleando el subcomando de router maximum-paths *número*.

Configuración de OSPF con una sola área

La configuración de OSPF sólo varía un poco respecto a la configuración de RIP cuando se utiliza una sola área OSPF. La mejor manera de describir la configuración y las dife-

rencias respecto a la configuración de otros protocolos de enrutamiento, consiste en utilizar un ejemplo. La Figura 9.7 muestra un ejemplo de red, y el Ejemplo 9.1 muestra la configuración de Albuquerque.

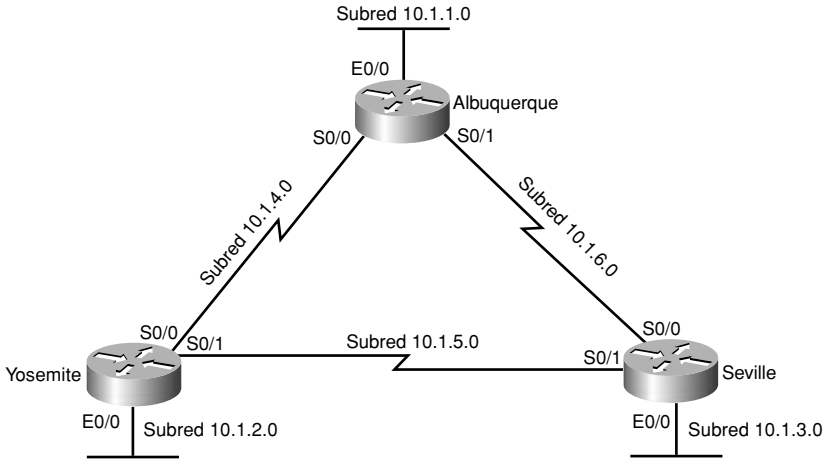


Figura 9.7. Ejemplo de red para una configuración de OSPF con una sola área.

Ejemplo 9.1. Configuración de OSPF con una sola área en Albuquerque.

```
interface ethernet 0/0
 ip address 10.1.1.1 255.255.255.0
interface serial 0/0
 ip address 10.1.4.1 255.255.255.0
interface serial 0/1
 ip address 10.1.6.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
```

La configuración habilita correctamente OSPF en las tres interfaces de Albuquerque. En primer lugar, el comando global `router ospf 1` pone al usuario en modo de configuración de OSPF. El comando `router ospf` tiene un parámetro denominado *id-proceso* de OSPF. En algunos casos, quizá se desee ejecutar múltiples procesos OSPF en un mismo router, así que el comando `router` hace uso de *id-proceso* para distinguir entre los procesos. El *id-proceso* no necesita ser el mismo en todos los routers y puede ser cualquier entero entre 1 y 65535.

El comando `network` indica al router que active OSPF en todas las interfaces indicadas, que busque vecinos de esa interfaz, que asigne la interfaz a un área, y que notifique la subred que está conectada a cada interfaz. En este caso, el comando `network 10.0.0.0 0.255.255.255 area 0` se refiere a las tres interfaces que tiene Albuquerque porque el comando OSPF `network` denota las interfaces empleando una dirección y una máscara

wildcard como las que se emplean con las ACLs IP. La máscara *wildcard* que se muestra en el Ejemplo 9.1 es 0.255.255.255, con la dirección 10.0.0.0. Tomando como base los detalles que se incluyen en el Capítulo 6, "Listas de control de acceso IP", esta combinación denota todas las direcciones que comienzan con un 10 como primer octeto. Por tanto, este único comando network denota las tres interfaces de Albuquerque, las pone en Área 0, y hace que Albuquerque intente descubrir vecinos de esas interfaces. Además, hace que Albuquerque notifique la existencia de las tres subredes que tiene conectadas.

La máscara *wildcard* del comando OSPF network se comporta como la máscara *wildcard* de una ACL, pero hay una restricción que afecta a los valores utilizados. La máscara *wildcard* OSPF debe tener una sola cadena de unos ("1") binarios consecutivos, y una sola cadena de ceros ("0") binarios consecutivos. Por ejemplo, una máscara de 0.0.255.255 representa 16 ceros binarios y 16 unos binarios, y sería admisible. De forma similar, una máscara de 255.255.255.0 sería admisible, porque tiene una cadena de 24 unos binarios seguida por una cadena de ocho ceros binarios. Sin embargo, un valor de 0.255.255.0 no sería admisible, porque tiene dos conjuntos de ocho ceros binarios, separados por una cadena de 16 unos binarios.

El Ejemplo 9.2 muestra una configuración alternativa para Albuquerque que también habilita OSPF en todas las interfaces. En este caso, la dirección IP de cada interfaz se trata mediante un comando network diferente. La máscara *wildcard* 0.0.0.0 significa que es preciso comparar los 32 bits, y que tienen que coincidir; por tanto, los comandos network incluyen la dirección IP de cada interfaz. Muchas personas prefieren este modo de configuración en las redes de producción, porque descarta toda posible ambigüedad relativa a las interfaces en las que se está ejecutando OSPF.

Ejemplo 9.2. Configuración OSPF de una sola área para Albuquerque, empleando tres comandos **network**.

```
interface ethernet 0/0
 ip address 10.1.1.1 255.255.255.0
interface serial 0/0
 ip address 10.1.4.1 255.255.255.0
interface serial 0/1
 ip address 10.1.6.1 255.255.255.0
!
router ospf 1
 network 10.1.1.1 0.0.0.0 area 0
 network 10.1.4.1 0.0.0.0 area 0
 network 10.1.6.1 0.0.0.0 area 0
```

Configuración de OSPF con múltiples áreas

La configuración de OSPF con múltiples áreas resulta sencilla cuando se comprende la configuración de OSPF en una sola área. Lo difícil es diseñar la red OSPF tomando decisiones correctas respecto a qué subredes deben ubicarse en qué áreas. Una vez terminado el

diseño de áreas, la configuración es sencilla. Por ejemplo, considérese la Figura 9.8, que muestra algunas subredes en Área 0 y algunas en Área 1.

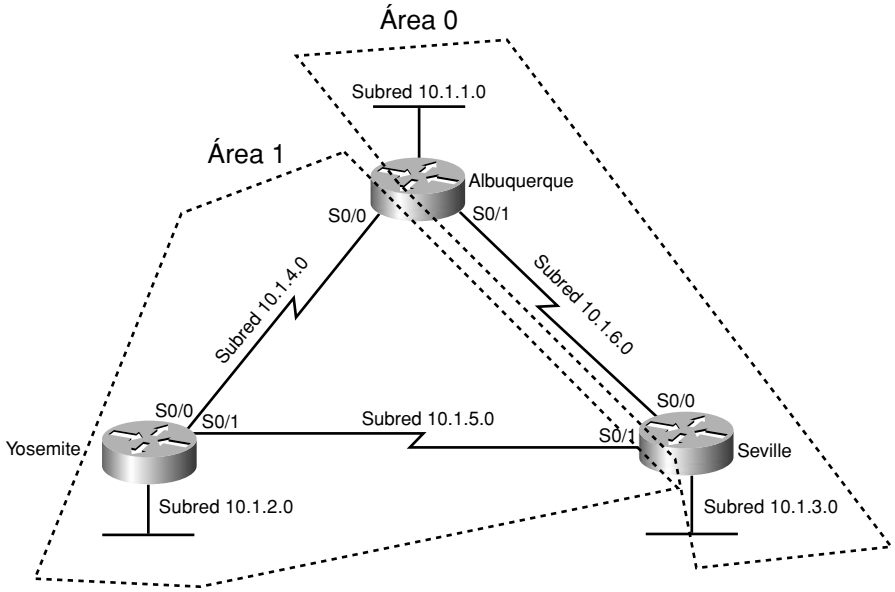


Figura 9.8. Una red OSPF con varias áreas.

En realidad, no se necesitan varias áreas en una red tan pequeña, pero se utilizan dos áreas en este ejemplo con objeto de mostrar la configuración. Obsérvese que Albuquerque y Seville son ambos ABR, pero Yosemite se halla totalmente dentro de Área 1, así que no es un ABR. Los Ejemplos 9.3 y 9.4 muestran la configuración de Albuquerque y Yosemite, junto con varios comandos show.

La configuración tiene que especificar el número de área correcto en las interfaces adecuadas. Por ejemplo, el comando network 10.1.4.1 0.0.0.0 area 1 que hay al principio del Ejemplo 9.3 se refiere a la dirección IP de la interfaz Serial 0/0 de Albuquerque, y pone esa interfaz en Área 1. Los comandos network 10.1.6.1 0.0.0.0 area 0 y network 10.1.1.1 0.0.0.0 area 0 ponen a las interfaces Serial 0/1 y Ethernet 0/0, respectivamente, en Área 0. A diferencia del Ejemplo 9.1, Albuquerque no se puede configurar para que coincida con las tres interfaces mediante un solo comando network, porque una de las interfaces (Serial 0/0) se encuentra en un área que es distinta del área de las otras dos.

Para continuar con el Ejemplo 9.3, el comando show ip route ospf se limita a enumerar las rutas que ha aprendido OSPF, en lugar de mostrar la tabla de enrutamiento IP completa. El comando show ip route muestra las tres rutas conectadas, así como las tres rutas aprendidas por OSPF. Obsérvese que la ruta de Albuquerque que va hacia 10.1.2.0 tiene la indicación O a su lado, lo cual denota **intra-área**, porque la subred reside en Área 1, y Albuquerque forma parte de Área 1 y de Área 0.

Ejemplo 9.3. Configuración de OSPF con varias áreas y comandos **show** en Albuquerque.

```
! Sólo se muestra la configuración de OSPF para ahorrar espacio
!
router ospf 1
 network 10.1.1.1 0.0.0.0 area 0
 network 10.1.4.1 0.0.0.0 area 1
 network 10.1.6.1 0.0.0.0 area 0
Albuquerque#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 6 subnets
O       10.1.3.0 [110/65] via 10.1.6.3, 00:01:04, Serial0/1
O       10.1.2.0 [110/65] via 10.1.4.2, 00:00:39, Serial0/0
C       10.1.1.0 is directly connected, Ethernet0/0
C       10.1.6.0 is directly connected, Serial0/1
O       10.1.5.0 [110/128] via 10.1.4.2, 00:00:39, Serial0/0
C       10.1.4.0 is directly connected, Serial0/0

Albuquerque#show ip route ospf
     10.0.0.0/24 is subnetted, 6 subnets
O       10.1.3.0 [110/65] via 10.1.6.3, 00:01:08, Serial0/1
O       10.1.2.0 [110/65] via 10.1.4.2, 00:00:43, Serial0/0
O       10.1.5.0 [110/128] via 10.1.4.2, 00:00:43, Serial0/0
```

Ejemplo 9.4. Configuración de OSPF con varias áreas y comandos **show** en Yosemite.

```
! Solo se muestra la configuración de OSPF para ahorrar espacio
router ospf 1
 network 10.0.0.0 0.255.255.255 area 1
Yosemite#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set
```

(continúa)

Ejemplo 9.4. Configuración de OSPF con varias áreas y comandos **show** en Yosemite *(continuación).*

```
    10.0.0.0/24 is subnetted, 6 subnets
IA      10.1.3.0 [110/65] via 10.1.5.1, 00:00:54, Serial0/1
IA      10.1.1.0 [110/65] via 10.1.4.1, 00:00:49, Serial0/0
C       10.1.2.0 is directly connected, Ethernet0/0
C       10.1.5.0 is directly connected, Serial0/1
IA      10.1.6.0 [110/128] via 10.1.4.1, 00:00:38, Serial0/0
C       10.1.4.0 is directly connected, Serial0/0
```

Obsérvese, en el Ejemplo 9.4, que la configuración OSPF de Yosemite sólo requiere un comando network porque todas las interfaces de Yosemite están en Área 1. Obsérvese también que las rutas aprendidas por Yosemite en los otros dos routers aparecen como rutas **interárea** (**IA**), porque esas dos subredes están en Área 0, y Yosemite está en Área 1.

Configuración del ID de router en OSPF

Los routers que utilizan OSPF necesitan tener un ID de router (RID) para funcionar correctamente. Para determinar el RID, los routers de Cisco emplean el proceso siguiente cuando el router se recarga y activa el proceso OSPF. Obsérvese que cuando uno de estos pasos identifica el RID, el proceso se detiene.

1. Si está configurado el comando router-id *rid* de OSPF, se utiliza ese valor como RID.
2. Si alguna de las interfaces *loopback* tiene configurada una dirección IP y la interfaz tiene el estado *up*/*up* para la línea y el protocolo, el router selecciona la dirección IP más alta numéricamente de entre las interfaces *loopback* que estén *up*/*up*.
3. El router selecciona la dirección IP más alta de entre todas las demás interfaces que estén en funcionamiento (*up*/*up*).

Los criterios primero y tercero deberían tener sentido a primera vista: el RID o bien se configura o se toma de la dirección IP de una interfaz operativa. Sin embargo, en este libro todavía no se ha explicado el concepto de **interfaz loopback**, que se menciona en el Paso 2. Una interfaz *loopback* es una interfaz virtual que se puede configurar mediante el comando interface loopback *número-de-interfaz*, donde *número-de-interfaz* es un entero. Las interfaces *loopback* siempre se encuentran en un estado "*up*/*up*" salvo que administrativamente se haga que pasen a un estado inactivo. Por ejemplo, una configuración sencilla del comando interface loopback 0, seguida por ip address 192.168.200.1 255.255.255.0, crearía una interfaz *loopback* y le asignaría una dirección IP. Como las interfaces *loopback* no se basan en hardware alguno, estas interfaces pueden estar *up*/*up* siempre que se esté ejecutando el IOS, lo cual hace de ellas unas buenas interfaces para tomarlas como base de un RID OSPF.

Cada router selecciona su RID OSPF cuando OSPF arranca. La inicialización se produce durante la carga inicial del IOS. Por tanto, si OSPF arranca y después se ponen en funcionamiento otras interfaces que tengan las direcciones IP más altas, entonces el RID OSPF no cambia mientras no se reinicie el proceso OSPF. OSPF puede reiniciarse también emple-

ando el comando clear ip ospf process, pero dependiendo de las circunstancias, el IOS quizá no modifique su RID OSPF hasta la próxima recarga del IOS.

Hay muchos comandos que enumeran la RID de OSPF en distintos routers. Por ejemplo, en el Ejemplo 9.5, el primer vecino que aparece en el resultado del comando show ip ospf neighbor es el Router ID 10.1.5.2, que es la RID de Yosemite. A continuación, show ip ospf indica la RID del propio Albuquerque.

Ejemplo 9.5. Visualización de información relacionada con OSPF en Albuquerque.

```
Albuquerque#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.6.3          1   FULL/  -        00:00:35    10.1.6.3        Serial0/1
10.1.5.2          1   FULL/  -        00:00:37    10.1.4.2        Serial0/0
Albuquerque#show ip ospf neighbor
Routing Process "ospf 1" with ID 10.1.6.1
! lines omitted for brevity
```

Temporizadores Hello y muerto de OSPF

La configuración predeterminada de los temporizadores Hello y Dead (muerto) de OSPF suelen funcionar perfectamente. Sin embargo, es importante observar que una discrepancia de cualquiera de estos ajustes puede dar lugar a que dos vecinos potenciales nunca lleguen a ser vecinos, puesto que no llegarán a alcanzar el estado bidireccional. El Ejemplo 9.6 muestra la forma más común de visualizar la configuración actual, empleando el comando show ip ospf interface en Albuquerque, que se ha configurado según se muestra en el ejemplo de OSPF para múltiples áreas (Ejemplos 9.3 y 9.4).

Ejemplo 9.6. Visualización de los temporizadores Hello y muerto en Albuquerque.

```
Albuquerque#show ip ospf interface
Serial0/1 is up, line protocol is up
  Internet Address 10.1.6.1/24, Area 0
  Process ID 1, Router ID 10.1.6.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 2/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.6.3
  Suppress hello for 0 neighbor(s)
```

(continúa)

Ejemplo 9.6. Visualización de los temporizadores Hello y muerto en Albuquerque *(continuación).*

```
Ethernet0/0 is up, line protocol is up
  Internet Address 10.1.1.1/24, Area 0
  Process ID 1, Router ID 10.1.6.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.6.1, Interface address 10.1.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0 is up, line protocol is up
  Internet Address 10.1.4.1/24, Area 1
  Process ID 1, Router ID 10.1.6.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.5.2
  Suppress hello for 0 neighbor(s)
```

Obsérvese también que el comando show ip ospf interface muestra una información más detallada sobre el funcionamiento de OSPF en cada interfaz. Por ejemplo, este comando muestra el número de área, el coste OSPF, y los vecinos conocidos en cada interfaz. Los temporizadores que se utilizan en la interfaz, incluyendo Hello y Dead, se muestran también.

Para configurar los intervalos Hello y Dead, se pueden utilizar los subcomandos de interfaz ip ospf hello-interval *valor* e ip ospf dead-interval *valor*. Curiosamente, si se configura el intervalo Hello, el IOS reconfigura automáticamente el intervalo Dead de la interfaz para que sea 4 veces el intervalo Hello.

Métrica de OSPF (coste)

OSPF calcula la métrica de cada posible ruta sumando los costes de las interfaces OSPF salientes. El coste OSPF de una interfaz se puede configurar, o bien lo puede calcular un router basándose en la configuración de ancho de banda de esa interfaz.

Como recordatorio, la configuración de ancho de banda de una interfaz se puede configurar empleando el subcomando de interfaz bandwidth. Este comando determina

la percepción que tiene el router de la velocidad de esa interfaz, empleando como unidades los Kbps. Obsérvese que no es necesario que la configuración de ancho de banda de la interfaz coincida con la velocidad física de la interfaz, pero normalmente tiene sentido que el ancho de banda especificado coincida con la velocidad física de la interfaz. En las interfaces Ethernet, el ancho de banda refleja la velocidad que se haya negociado en ese momento: 10.000 (que significa 10.000 Kbps o 10 Mbps) para redes Ethernet de 10 Mbps, y 100.000 (que significa 100.000 Kbps o 100 Mbps) para redes a 100 Mbps. Para las interfaces serie, el ancho de banda tiene un valor predeterminado de 1544 (que significa 1544 Kbps, o velocidad T1), pero el IOS no puede ajustar este valor dinámicamente.

El IOS selecciona el coste de una interfaz basándose en las reglas siguientes:

1. El coste se puede fijar explícitamente empleando el subcomando de interfaz `ip ospf cost x`, con un valor que puede oscilar entre 1 y 65.535, ambos inclusive.
2. El IOS puede calcular un valor basado en la fórmula general *Ref-BW* / *Int-BW*, donde *Ref-BW* es un ancho de banda de referencia que tiene un valor predeterminado de 100 Mbps, e *Int-BW* es la configuración de ancho de banda de la interfaz.
3. Se puede configurar el ancho de banda de referencia con valores distintos del predeterminado (100 Mbps) empleando el subcomando OSPF de router `auto-cost reference-bandwidth ref-bw`, que a su vez afectará al cálculo del ancho de banda predeterminado de la interfaz.

La sencilla fórmula que se emplea para calcular el coste OSPF predeterminado tiene un aspecto que podría inducir a confusión. El cálculo requiere que el numerador y el denominador utilicen las mismas unidades, pero los comandos `bandwidth` y `auto-cost reference-bandwidth` emplean unidades distintas. Por ejemplo, el software IOS de Cisco aplica a las interfaces Ethernet un ancho de banda predeterminado de 10.000, que significa 10.000 Kbps o 10 Mbps. El ancho de banda de referencia tiene un valor predeterminado de 100, que significa 100 Mbps. Por tanto, el coste OSF predeterminado de una interfaz Ethernet sería de 100 Mbps / 10 Mbps, después de conseguir que ambos valores utilicen Mbps como unidad. Las interfaces serie de velocidades más elevadas tienen un ancho de banda predeterminado de 1544, lo cual produce un coste predeterminado de 10^8 bps / 1.544.000 bps, que se redondea a la baja para dar un valor de 64, según se muestra para la interfaz S0/1 en el Ejemplo 9.6. Si el ancho de banda de referencia se hubiera modificado al valor 1000, empleando el subcomando OSPF de router `auto-cost reference-bandwidth 1000`, la métrica calculada sería 647.

El motivo principal para cambiar el ancho de banda de referencia es que los routers puedan tener distintos costes para la interfaces que funcionen a velocidades de 1000 Mbps y más. Con la configuración predeterminada, una interfaz que tenga una configuración de ancho de banda de 100 Mbps (por ejemplo, una interfaz FE) y una interfaz que tenga un ancho de banda de 1000 Mbps (por ejemplo, una interfaz GE) tendrían ambas un coste predeterminado igual a 1. Al modificar el ancho de banda de referencia a 1000, que denota 1000 Mbps, el coste predeterminado de una interfaz con un ancho de banda de 100 Mbps sería de 10, frente a un coste predeterminado de 1 en una interfaz cuyo ancho de banda fuera de 1000 Mbps.

NOTA

Cisco recomienda que la configuración de ancho de banda de referencia OSPF sea la misma en todos los routers OSPF de una red.

Autenticación en OSPF

La autenticación es probablemente la más importante de las características opcionales de configuración en OSPF. La falta de autenticación abre la red a ataques en que un atacante conecta un router a la red y los routers legítimos creen que son ciertos los datos OSPF procedentes del router pirata. Como resultado, el atacante puede producir fácilmente un ataque por denegación de servicio (DoS) haciendo que todos los routers descarten rutas legítimas que van a todas las subredes, e instalar en su lugar rutas que reenvían paquetes al router atacante. El atacante también puede efectuar un reconocimiento, y obtener información de la red poniéndose a la escucha de mensajes OSPF e interpretándolos.

OSPF admite tres tipos de autenticación: uno denominado autenticación nula (lo cual quiere decir que no hay autenticación), uno que emplea una simple contraseña de texto y que por tanto es fácil de violar, y uno que utiliza MD5. Francamente, si uno va a molestarse en configurar una opción en una situación real, la opción MD5 es la única opción razonable. En cuanto un router ha configurado la autenticación OSPF en una interfaz, ese router tiene que pasar el proceso de autenticación para todos los mensajes OSPF que intercambie con routers vecinos a través de esa interfaz. Esto significa que los routers vecinos de esa interfaz también tienen que tener el mismo tipo de autenticación, y la misma contraseña de autenticación.

La configuración puede utilizar dos subcomandos de interfaz en cada interfaz, uno para activar un tipo concreto de autenticación, y otro para establecer la contraseña que se utilizará en la autenticación.

El Ejemplo 9.7 muestra un caso de configuración en el que se especifica una sencilla autenticación por contraseña en la interfaz Fa0/0, y una autenticación MD5 en la interfaz Fa0/1.

Ejemplo 9.7. Autenticación OSPF empleando únicamente subcomandos de interfaz.

```
! Los comandos siguientes activan la autenticación sencilla mediante contraseñas
! en OSPF y establecen la contraseña al valor "key-t1".
R1#show running-config
! Se han omitido líneas para abreviar
interface FastEthernet0/0
 ip ospf authentication
 ip ospf authentication-key key-t1
! Formada la relación de vecindad, la autenticación funciona.
R1# show ip ospf neighbor fa 0/0
```

(continúa)

Ejemplo 9.7. Autenticación OSPF empleando únicamente subcomandos de interfaz *(continuación).*

```
Neighbor ID      Pri    State        Dead Time   Address         Interface
2.2.2.2          1      FULL/BDR     00:00:37    10.1.1.2        FastEthernet0/0
! Ahora, en la última o dos últimas líneas de la salida del
! comando de interfaz show ip ospf puede verse el tipo de
! autenticación ospf de cada interfaz
R1# show ip ospf interface fa 0/0
! Se han omitido líneas para abreviar
 Simple password authentication enabled

! Abajo, la interfaz Fa 0/1 de R1 está configurada para utilizar
! la autenticación de tipo 2. La clave debe definirse
! con el subcomando de interfaz ip ospf message-digest-key.
R1#show running-config
! Se han omitido líneas para abreviar
interface FastEthernet0/1
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 key-t2
! Este comando confirma la autenticación de tipo 2 (MD5), número clave 1.
R1# show ip ospf interface fa 0/1
! Se han omitido líneas para abreviar
Message digest authentication enabled
Youngest key id is 1
```

La parte más complicada de la configuración consiste en recordar la sintaxis de los comandos que se utilizan en los dos subcomandos de interfaz. Obsérvense los subcomandos de interfaz que se emplean para configurar las claves de autenticación, con una sintaxis que difiere dependiendo del tipo de autenticación. Como referencia, la Tabla 9.4 muestra los tres tipos de autenticación OSPF y los comandos correspondientes.

Tabla 9.4. Tipos de autenticación OSPF.

Tipo	Indica	Comando para habilitar la autenticación	Configuración de la contraseña
0	Nada	ip ospf authentication null	—
1	Texto puro	ip ospf authentication	ip ospf authentication-key *valor-clave*
2	MD5	ip ospf authentication message-digest	ip ospf message-digest-key *número-clave* md5 *valor-clave*

Obsérvese que las contraseñas o claves de autenticación se mantienen en forma de texto sin formato en la configuración, salvo que se añada el comando global service password-encryption a la configuración. (Si tiene una copia del libro **CCENT/CCNA ICND1**, puede consultar el Capítulo 9 si desea más información relativa al comando service password-encryption.)

La configuración predeterminada, que es de tipo 0 (no utilizar autenticación), se puede rescindir área por área empleando el comando de router area authentication. Por ejemplo, el Router R1 del Ejemplo 9.7 se podría configurar empleando un subcomando de router area 1 authentication message-digest, que hace que ese router pase a utilizar de forma predeterminada la autenticación MD5 en todas sus interfaces de Área 1. De forma similar, el subcomando de router area 1 authentication activa la autenticación simple por contraseña en todas las interfaces de Área 1, haciendo innecesario el comando ip ospf authentication. Obsérvese que las claves de autenticación (las contraseñas) aún deben ser configuradas mediante los comandos de subinterfaz que se enumeran en la Tabla 9.4.

Equilibrado de la carga en OSPF

Cuando OSPF utiliza SPF para calcular la métrica de las distintas rutas que llevan a una subred, una ruta puede tener la métrica más baja, de modo que OSPF la pone en la tabla de enrutamiento. Sin embargo, cuando se produce un empate entre las métricas, el router puede poner hasta 16 rutas distintas de igual coste en la tabla de enrutamiento (de forma predeterminada, se ponen hasta cuatro rutas distintas) basándose en el valor que tenga el subcomando de router maximum-paths *número*. Por ejemplo, si una red tuviera seis posibles rutas entre ciertas partes de la red, y el ingeniero quisiera que se utilizasen todas las rutas, se podrían configurar los routers mediante el subcomando maximum-paths 6 bajo router ospf.

El concepto más complejo está relacionado con la forma en que los routers utilizan múltiples rutas. Un router puede efectuar un equilibrado de la carga considerando cada paquete individual. Por ejemplo, si un router tuviera tres rutas OSPF de igual coste para una misma subred en la tabla de enrutamiento, el router podría enviar el próximo paquete a través de la primera ruta, el siguiente a través de la segunda ruta, el siguiente a través de la tercera ruta, y después volver a empezar en la primera ruta para el paquete siguiente. Alternativamente, el equilibrado de la carga se podría hacer por cada dirección IP de destino.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 9.5 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 9.5. Temas claves del Capítulo 9.

Tema clave	Descripción	Número de página
Lista	Ajustes que deben coincidir en los vecinos OSPF para que puedan hacerse vecinos y llegar al estado bidireccional (por lo menos).	347
Figura 9.2	Estados de vecindad y mensajes que se intercambian en la formación de vecinos OSPF.	348
Lista	Resumen en tres pasos del proceso de intercambio de la base de datos topológica en OSPF.	350
Figura 9.3	Dibujo que compara las adyacencias completas que se forman con y sin un DR.	350
Lista	Reglas para seleccionar un router designado.	351-352
Tabla 9.2	Estados de vecindad OSPF y sus significados.	353
Lista	Lista de razones por las cuales OSPF necesita áreas para crecer correctamente.	356
Tabla 9.3	Términos y definiciones de diseño en OSPF.	357
Lista	Lista de comprobación para la configuración en OSPF.	359
Lista	Detalles de la forma en que el IOS determina el coste OSPF de una interfaz.	364
Tabla 9.4	Tipos de autenticación OSPF y comandos de configuración.	369

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD), o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas ya completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe sus respuestas en el glosario:

Actualización de estado del enlace, base de datos topológica, completamente adyacente, descripción de base de datos, Estado bidireccional, estado *Full*, ID de router (RID), intervalo Hello, intervalo muerto, notificación del estado del enlace, router designado, Router designado de respaldo,Router fronterizo (ABR), Router fronterizo de sistema autónomo (ASBR), solicitud de estado del enlace, tabla de vecinos, vecino.

Referencias de comandos

Aunque no es necesario memorizar la información de las tablas de esta sección, se incluye una referencia de los comandos de configuración y EXEC que se han tratado en este capítulo. Desde un punto de vista práctico, debería aprender de memoria los comandos a medida que va leyendo el capítulo y haciendo todas las actividades de esta sección de preparación del examen. Para ver hasta qué punto ha memorizado los comandos como efecto secundario de su estudio, lea las descripciones que hay en el lado derecho e intente recordar el comando que debe aparecer a la izquierda.

Tabla 9.6. Comandos de configuración del Capítulo 9.

Comando	Descripción
router ospf *id-proceso*	Entra en el modo de configuración OSPF para el proceso indicado.
network *dirección-ip máscara-*wildcard area *id-área*	Subcomando de router que activa OSPF en las interfaces indicadas por la combinación de dirección y *wildcard*, y que además establece el área OSPF.

(continúa)

Tabla 9.6. Comandos de configuración del Capítulo 9 *(continuación)*.

Comando	Descripción
ip ospf cost *coste-interfaz*	Subcomando de interfaz que especifica el coste OSPF asociado a la interfaz.
bandwidth *ancho-de-banda*	Subcomando de interfaz que establece directamente el ancho de banda de la interfaz (en Kbps).
auto-cost reference- bandwidth *número*	Subcomando de router que proporciona a OSPF el numerador de la fórmula Ref-BW/ Int-BW que se utiliza para calcular el coste OSPF en base al ancho de banda de la interfaz.
ip ospf hello *número*	Subcomando de interfaz que establece el intervalo Hello de OSPF, y que además reinicia el intervalo Dead a 4 veces este número.
ip ospf dead-interval *número*	Subcomando de interfaz que establece el temporizador muerto de OSPF.
ip ospf network *tipo*	Subcomando de interfaz que define el tipo de red OSPF.
router-id *id*	Comando OSPF que establece de forma estática el ID del router.
ip ospf hello-interval *segundos*	Subcomando de interfaz que fija el intervalo de los Hellos periódicos.
ip ospf priority *valor-numérico*	Subcomando de interfaz que fija la prioridad OSPF de una interfaz.
maximum-paths *número-de-rutas*	Subcomando de router que define el número máximo de rutas de igual coste que se pueden añadir a la tabla de enrutamiento.
ip ospf authentication [null | message-digest]	Subcomando de interfaz que activa una autenticación de tipo 0 (null), de tipo 1 (no se muestra el parámetro opcional), o de tipo 2 (message-digest).
ip ospf message-digest-key *número-clave* md5 *valor-clave*	Subcomando de interfaz que establece la clave de autenticación OSPF si se emplea la autenticación MD5.
ip ospf authentication *valor-clave*	Subcomando de interfaz que establece la clave de autenticación OSPF si se emplea una autenticación de contraseña simple.
area *área* authentication [message-digest | null]	Subcomando de router que configura el servicio de autenticación predeterminado para las interfaces del área indicada.

Tabla 9.7. Comandos EXEC del Capítulo 9.

Comando	Descripción
show ip route ospf	Muestra las rutas de la tabla de enrutamiento que se han aprendido mediante OSPF.
show ip protocols	Muestra los parámetros del protocolo de enrutamiento y los valores actuales de los temporizadores.
show ip ospf interface	Muestra el área en que reside la interfaz, los vecinos adyacentes en esta interfaz y los temporizadores Hello y Dead.
show ip ospf neighbor [*RID-vecino*]	Muestra los vecinos y el estado actual de esta interfaz respecto a los vecinos; opcionalmente, muestra los detalles del ID de router indicado en el comando.
debug ip ospf events	Emite mensajes de registro para cada paquete OSPF.
debug ip ospf packet	Emite mensajes de registro que describen el contenido de todos los paquetes OSPF.
debug ip ospf hello	Emite mensajes de registro que describen los mensajes Hello y sus fallos.

Este capítulo trata los siguientes temas:

Conceptos y funcionamiento de EIGRP: Esta sección explica los conceptos que subyacen a los vecinos EIGRP, al intercambio de información topológica y al cálculo de rutas.

Configuración y verificación de EIGRP: Esta sección muestra la forma de configurar EIGRP, incluyendo la autenticación y el ajuste fino de la métrica, así como la forma de determinar las rutas del sucesor y del sucesor viable en la salida de los comandos show.

CAPÍTULO 10

EIGRP

El Protocolo de enrutamiento de gateway interno mejorado (*Enhanced Interior Gateway Routing Protocol*, EIGRP) ofrece una notable colección de características y atributos adecuados para su propósito principal, que es aprender rutas IP. EIGRP converge de manera muy rápida, tanto o más que OSPF, pero sin algunos de los aspectos negativos de OSPF. En particular, EIGRP requiere mucho menos tiempo de procesamiento, mucha menos memoria, y mucho menos esfuerzo de diseño que OSPF. El único aspecto negativo de importancia es que EIGRP es propiedad de Cisco, luego si una red hace uso de routers que no sean de Cisco, no será posible utilizar EIGRP en esos routers.

EIGRP no encaja exactamente en las categorías generales de protocolos de enrutamiento por vector de distancia y por estado del enlace. En algunas ocasiones, Cisco hace alusión a EIGRP como si se tratara simplemente de un protocolo avanzado por vector de distancia, pero en otros casos Cisco se refiere a EIGRP como a un nuevo tipo: un protocolo de enrutamiento híbrido equilibrado. Independientemente de la categoría, los conceptos y los procesos subyacentes que emplea EIGRP pueden tener algunas similitudes con otros protocolos de enrutamiento, pero son muchas más las diferencias, lo cual hace de EIGRP un protocolo de enrutamiento único en sí mismo.

Este capítulo comienza examinando algunos de los conceptos clave que subyacen a la forma en que funciona EIGRP. La segunda mitad del capítulo explica la configuración y verificación de EIGRP.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las nueve preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 10.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

Tabla 10.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
Conceptos y funcionamiento de EIGRP	1-4
Configuración y verificación de EIGRP	5-9

1. ¿Cuáles de los factores siguientes afectan al cálculo de métricas EIGRP cuando se utilizan todos los valores predeterminados posibles?
   - **a.** Ancho de banda.
   - **b.** Retardo.
   - **c.** Carga.
   - **d.** Fiabilidad.
   - **e.** MTU.
   - **f.** Número de saltos.
2. ¿Cómo se entera EIGRP de que ha fallado un router vecino?
   - **a.** El vecino que falla envía un mensaje antes de fallar.
   - **b.** El vecino que falla envía un mensaje de "último suspiro".
   - **c.** El router observa una falta de actualizaciones de enrutamiento durante un cierto periodo de tiempo.
   - **d.** El router observa una carencia de mensajes Hello durante un cierto periodo de tiempo.
3. ¿Cuáles de las siguientes afirmaciones son ciertas respecto al concepto de distancia factible en EIGRP?
   - **a.** La distancia factible de una ruta es la métrica calculada de una ruta sucesora factible.
   - **b.** La distancia factible de una ruta es la métrica calculada de una ruta sucesora.
   - **c.** La distancia factible es la métrica de una ruta desde la perspectiva de un router vecino.
   - **d.** La distancia factible es la métrica EIGRP asociada a cada posible ruta para alcanzar una subred.
4. ¿Cuáles de las siguientes afirmaciones son ciertas respecto al concepto de distancia informada en EIGRP?
   - **a.** La distancia informada de una ruta es la métrica calculada de una ruta sucesora factible.
   - **b.** La distancia informada de una ruta es la métrica calculada de la ruta sucesora.
   - **c.** La distancia informada de una ruta es la métrica de una ruta desde la perspectiva de un router vecino.

d. La distancia informada es la métrica EIGRP asociada a cada posible ruta para alcanzar una subred.

5. ¿Cuál de los siguientes comandos network, que siguen al comando router eigrp 1, indica a este router que empiece a utilizar EIGRP en las interfaces cuyas direcciones IP son 10.1.1.1, 10.1.100.1, 10.1.120.1?

a. network 10.0.0.0

b. network 10.1.1x.0

c. network 10.0.0.0 0.255.255.255

d. network 10.0.0.0 255.255.255.0

6. Los routers R1 y R2 se conectan a la misma VLAN con las direcciones IP 10.0.0.1 y 10.0.0.2, respectivamente. R1 se ha configurado con los comandos router eigrp 99 y network 10.0.0.0. ¿Cuál de los siguientes comandos podría formar parte de una configuración EIGRP operativa para R2 que asegurase que ambos routers se harían vecinos e intercambiarían rutas?

a. network 10

b. router eigrp 98

c. network 10.0.0.2 0.0.0.0

d. network 10.0.0.0

7 Examine el siguiente fragmento de la CLI de un router:

```
P 10.1.1.0/24, 1 successors, FD is 2172416
         via 10.1.6.3 (2172416/28160), Serial0/1
         via 10.1.4.2 (2684416/2284156), Serial0/0
         via 10.1.5.4 (2684416/2165432), Serial1/0
```

¿Cuál de las siguientes opciones identifica una dirección IP de siguiente salto en una ruta sucesora factible?

a. 10.1.6.3

b. 10.1.4.2

c. 10.1.5.4

d. No se puede determinar a partir de la salida de este comando.

8. ¿Qué debe ocurrir para configurar la autenticación MD5 para EIGRP?

a. Hay que establecer la clave de autenticación MD5 mediante algun subcomando de interfaz.

b. Hay que configurar al menos una cadena de clave.

c. Hay que definir una duración válida para la clave.

d. Hay que habilitar la autenticación EIGRP MD5 en una interfaz.

9. En el comando show ip route, ¿qué indicación de código implica que una ruta se ha aprendido a través de EIGRP?

a. E
b. I
c. G
d. R
e. P
f. D

Temas fundamentales

Conceptos y funcionamiento de EIGRP

Al igual que OSPF, EIGRP sigue tres pasos generales para poder añadir rutas a la tabla de enrutamiento IP:

1. **Descubrimiento de vecinos**: los routers EIGRP envían mensajes Hello para descubrir routers EIGRP vecinos potenciales, y realizan comprobaciones básicas de los parámetros para determinar qué routers deberían pasar a ser vecinos.
2. **Intercambio de topologías**: los vecinos pueden intercambiar actualizaciones completas de topología cuando se establece una relación de vecindad; en lo sucesivo, sólo se precisarán actualizaciones parciales, basadas en los cambios que haya en la topología de la red.
3. **Selección de rutas**: cada router analiza sus respectivas tablas de topología EIGRP, y selecciona la ruta de métrica más baja para llegar a cada subred.

Como resultado de estos tres pasos, el IOS mantiene tres tablas EIGRP importantes. La tabla de vecinos EIGRP contiene los routers de la vecindad y se visualiza mediante el comando `show ip eigrp neighbor`. La tabla de topología EIGRP contiene toda la información topológica que se ha aprendido de los vecinos EIGRP y se visualiza mediante el comando `show ip eigrp topology`. Por último, la tabla de enrutamiento IP contiene todas las mejores rutas y se visualiza mediante el comando `show ip route`.

Las próximas secciones describen algunos detalles relativos a la forma en que EIGRP establece relaciones de vecindad, intercambia rutas y añade entradas a la tabla de enrutamiento IP. Además de estos tres pasos, esta sección explica cierta lógica exclusiva que utiliza EIGRP cuando converge y reacciona frente a cambios en una red; esta lógica no se observa en otros tipos de protocolos de enrutamiento.

Vecinos EIGRP

Los vecinos EIGRP son otros routers que utilizan EIGRP y están conectados a una subred común, con los que el router está dispuesto a intercambiar información topológica

de EIGRP. EIGRP utiliza mensajes Hello de EIGRP, que se envían a la dirección IP de multidifusión 224.0.0.10, con objeto de descubrir dinámicamente vecinos potenciales. El router conoce a sus vecinos potenciales cuando recibe un Hello.

Los routers efectúan una comprobación básica de cada vecino potencial antes de que el otro router llegue a ser un vecino EIGRP. Un vecino potencial es un router del cual se ha recibido un Hello EIGRP. Entonces el router verifica los ajustes siguientes para determinar si se debe permitir al router que llegue a ser un vecino:

- Debe pasar el proceso de autenticación.
- Debe utilizar el mismo número AS configurado.
- La dirección IP de origen empleada por el Hello del vecino debe estar en la misma subred.

Nota

Los valores K EIGRP en ambos routers también tienen que coincidir, pero esta cuestión va más allá de los límites de este libro.

Las comprobaciones de verificación son relativamente sencillas. Si está configurada la autenticación, los dos routers tienen que estar empleando el mismo tipo de autenticación y la misma clave de autenticación. La configuración de EIGRP contiene un parámetro llamado número de sistema autónomo (ASN), que tiene que ser el mismo en los dos routers vecinos. Por último, las direcciones IP empleadas para enviar mensajes Hello de EIGRP (las respectivas direcciones IP de las interfaces de los routers) tienen que estar dentro del intervalo de direcciones de la subred a que esté conectado el otro router.

La relación de vecindad EIGRP es mucho más sencilla que la de OSPF. EIGRP no tiene un concepto adicional de ser completamente adyacente, como ocurre en OSPF, y tampoco hay estados de vecindad como los de OSPF: en cuanto se descubre un vecino EIGRP y pasa las comprobaciones de verificación básicas, el router pasa a ser un vecino. A partir de ese momento, los dos routers pueden empezar a intercambiar información topológica. Los vecinos envían mensajes Hello a cada intervalo Hello de EIGRP. Un router considera que un vecino EIGRP ya no está disponible cuando no se producen mensajes Hello del vecino durante el número de segundos definido por el temporizador Hold (espera) de EIGRP, que viene a ser parecido al intervalo muerto de OSPF.

Intercambio de información topológica en EIGRP

EIGRP hace uso de **mensajes de actualización** EIGRP para enviar información topológica a los vecinos. Estos mensajes de actualización se pueden enviar a la dirección IP de multidifusión 224.0.0.10 si el router remitente necesita actualizar múltiples routers de la

misma subred; en caso contrario, las actualizaciones se envían a la dirección IP de unidifusión de ese vecino en particular. (Los mensajes Hello siempre se envían a la dirección de multidifusión 224.0.0.10.) A diferencia de OSPF, no existe el concepto de Router designado (DR) ni el de Router designado de respaldo (BDR), pero el uso de paquetes de multidifusión en las LANs permite a EIGRP intercambiar información topológica con todos los vecinos de la LAN de forma eficiente.

Los mensajes de actualización se envían empleando el Protocolo de transporte fiable (*Reliable Transport Protocol*, RTP). La importancia de RTP consiste en que, igual que OSPF, EIGRP vuelve a enviar las actualizaciones de enrutamiento que se pierden en tránsito. Al utilizar RTP, EIGRP puede evitar mejor los bucles.

Nota

El acrónimo RTP también denota otro protocolo distinto, el Protocolo de transporte en tiempo real (*Real-time Transport Protocol*, RTP), que se utiliza para transmitir paquetes IP de voz y vídeo.

Los vecinos utilizan tanto actualizaciones completas de enrutamiento como actualizaciones parciales, según se muestra en la Figura 10.1. Las actualizaciones completas quieren decir que un router envía información relativa a todas las rutas conocidas, mientras que en una actualización parcial sólo se incluyen las rutas que hayan cambiado recientemente. Las actualizaciones completas se producen cuando los vecinos se activan por primera vez. En lo sucesivo, los vecinos sólo envían actualizaciones parciales como reacción frente a cambios de alguna ruta. Desde la parte superior a la inferior, la Figura 10.1 muestra el descubrimiento de vecinos mediante mensajes Hello, el envío de actualizaciones completas, el mantenimiento de la relación de vecindad mediante mensajes Hello sucesivos, y las actualizaciones parciales.

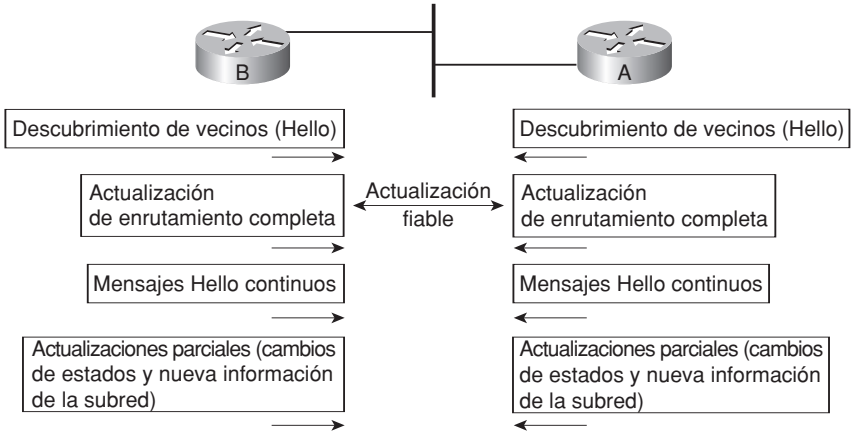


Figura 10.1. Actualizaciones EIGRP totales y parciales.

Cálculo de las mejores rutas para la tabla de enrutamiento

El cálculo de métricas es una de las características más interesantes de EIGRP. Este protocolo utiliza una métrica compuesta, que se calcula de forma predeterminada como una función del ancho de banda y del retardo. El cálculo también puede tener en cuenta la carga de la interfaz y su fiabilidad, aunque Cisco recomienda no utilizarlas. EIGRP calcula la métrica de cada posible ruta insertando en una fórmula los valores de la métrica compuesta.

Nota

Los documentos y libros anteriores solían decir que EIGRP, así como su predecesor, IGRP, podían utilizar la MTU como parte de la métrica, pero MTU no se puede utilizar y nunca se ha considerado que formara parte del cálculo.

La fórmula de cálculo de la métrica en EIGRP ayuda a describir algunos de los puntos clave de la métrica. La fórmula, suponiendo que los ajustes predeterminados utilicen nada más el ancho de banda y el retardo, es como sigue:

$$\text{Métrica} = \left(\left(\frac{10^7}{\text{ancho-de-banda-mínimo}} \right) + \text{retardo — acumulado} \right) * 256$$

En esta fórmula, el término *ancho-de-banda-mínimo* representa el del enlace de ancho de banda más pequeño de la ruta, en kbps. Por ejemplo, si el enlace más lento de una ruta es un enlace Ethernet de 10 Mbps, entonces la primera parte de la fórmula será 10^7 / 10^4, que es igual a 1000. En la fórmula se utiliza 10^4 porque 10 Mbps es igual a 10000 kbps (10^4 kbps). El valor del retardo acumulado que se emplea en la fórmula es la suma de los valores de todos los retardos que haya en todos los enlaces de la ruta, empleando como unidades las "decenas de microsegundos". Se puede especificar tanto el ancho de banda como el retardo de cada enlace empleando unos subcomandos de interfaz llamados, muy apropiadamente, bandwidth y delay.

Nota

La mayoría de los comandos show, incluyendo show ip eigrp topology y show interfaces, indican los ajustes de retardo como el número de microsegundos de retardo. La fórmula de la métrica emplea como unidad las decenas de microsegundos.

Las actualizaciones de EIGRP contienen el número de subred y la máscara, junto con el retardo acumulado, el ancho de banda mínimo y otras partes de la métrica compuesta que normalmente no se usan. Entonces el router considera los ajustes de ancho de banda y de retardo de la interfaz respecto a la cual se ha recibido una actualización, y calcula una nue-

va métrica. Por ejemplo, en la Figura 10.2 se muestra a Albuquerque aprendiendo sobre la subred 10.1.3.0/24 a partir de Seville. La actualización muestra un ancho de banda mínimo de 100000 kbps, y un retardo acumulado de 100 microsegundos. R1 posee un ancho de banda de interfaz establecido a 1544 kbps (el ancho de banda predeterminado de un enlace serie) y un retardo de 20000 microsegundos.

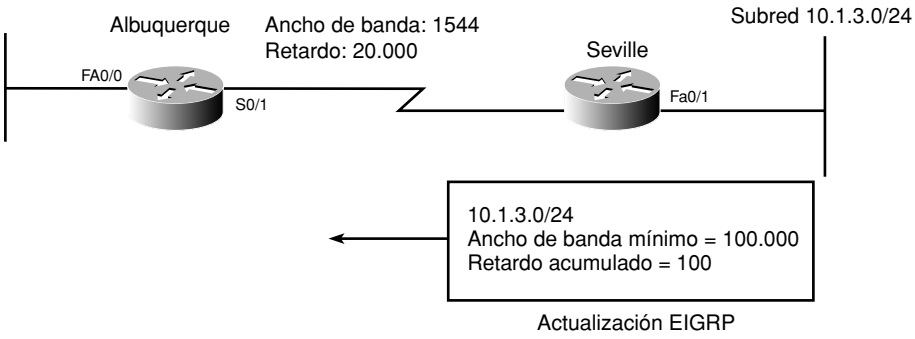


Figura 10.2. Forma en que Albuquerque calcula su métrica EIGRP para 10.1.3.0/24.

En este caso, Albuquerque descubre que el ancho de banda de su interfaz S0/1 (1544) es menor que el ancho de banda mínimo publicado, que es de 100000, así que Albuquerque utiliza este ancho de banda nuevo (y menor) en el cálculo de la métrica. (Si la interfaz S0/1 tuviera un ancho de banda de 100000 o más en este caso, Albuquerque utilizaría en su lugar el ancho de banda mínimo indicado en la actualización EIGRP procedente de Seville.) Albuquerque también añade el retardo de la interfaz S0/1 (20.000 microsegundos, transformados en 2000 decenas de microsegundos para la fórmula) al retardo acumulado recibido de Seville en la actualización (100 microsegundos, convertidos en 10 decenas de microsegundos). Esto da lugar al siguiente cálculo para la métrica:

$$\text{Métrica} = \left(\left(\frac{10^7}{1544}\right) + (10 + 2000)\right) * 256 = 2.172.416$$

Nota

El IOS redondea la división hacia abajo, para obtener el entero más próximo antes de calcular el resto de la fórmula. En este caso, 10^7 / 1544 se redondea a la baja para dar 6476.

Si existieran múltiples rutas posibles para llegar a la subred 10.1.3.0/24, Albuquerque también calcularía la métrica de esas rutas y seleccionaría la ruta que tuviera la mejor métrica (la más baja) para añadirla a la tabla de enrutamiento. Si hay un empate entre métricas, de forma predeterminada el router pondrá hasta cuatro rutas de igual métrica en

la tabla de enrutamiento, y enviará parte del tráfico a través de cada una de las rutas. La última sección, "Rutas máximas y varianza en EIGRP", explica algunos detalles más respecto a la forma en que EIGRP puede añadir múltiples rutas de igual métrica, y múltiples rutas de métricas desiguales a la tabla de enrutamiento.

Distancia factible y distancia informada

El ejemplo descrito en la Figura 10.2 ofrece una imagen de fondo muy adecuada para definir un par de términos EIGRP:

- **Distancia factible (*Feasible Distance*, FD)**: Es la métrica de la mejor ruta para llegar a una subred, tal como se ha calculado en un router.
- **Distancia informada o notificada (*Reported Distance*, RD)**: Es la métrica tal como se ha calculado en un router vecino, para después ser notificada y aprendida en una actualización EIGRP.

Por ejemplo, en la Figura 10.2 Albuquerque calcula una FD de 2.195.631 para llegar a la subred 10.1.3.0/24 a través de Seville. Seville también calcula su propia métrica para llegar a la subred 10.1.3.0/24. Seville también muestra esa métrica en la actualización EIGRP que envía a Albuquerque. De hecho, basándose en la información de la Figura 10.2, la FD de Seville para llegar hasta la subred 10.1.3.0/24, que después conocerá Albuquerque como RD de Seville para llegar a la subred 10.1.3.0/24, se puede calcular fácilmente:

$$\left(\left(\frac{10^7}{100.000}\right) + (10)\right) * 256 = 28.160$$

FD y RD se mencionan en una descripción próxima de la forma en que reacciona y converge EIGRP cuando se produce un cambio en una red.

Precauciones relativas al ancho de banda en enlaces serie

La robusta métrica de EIGRP le da la capacidad de seleccionar rutas que incluyan más saltos de router, pero con enlaces más rápidos. Para asegurar que sean seleccionadas las rutas correctas, los ingenieros deben tener cuidado a la hora de configurar unos ajustes significativos para el ancho de banda y para el retardo. En particular, los enlaces serie tienen un ancho de banda predeterminado de 1544 y un retardo de 20000 microsegundos, que es lo que se ha utilizado en el ejemplo de la Figura 10.2. Sin embargo, el IOS no puede cambiar automáticamente los ajustes de ancho de banda y de retardo basándose en la velocidad de capa 1 de un enlace serie. Por tanto, utilizar los valores predeterminados de ancho de banda en un enlace serie puede dar lugar a problemas.

La Figura 10.3 muestra el problema que surge al emplear la configuración predeterminada de ancho de banda y cómo EIGRP emplea la ruta mejor (la más rápida) cuando se configura correctamente el ancho de banda. La figura se centra en la ruta del router B hacia

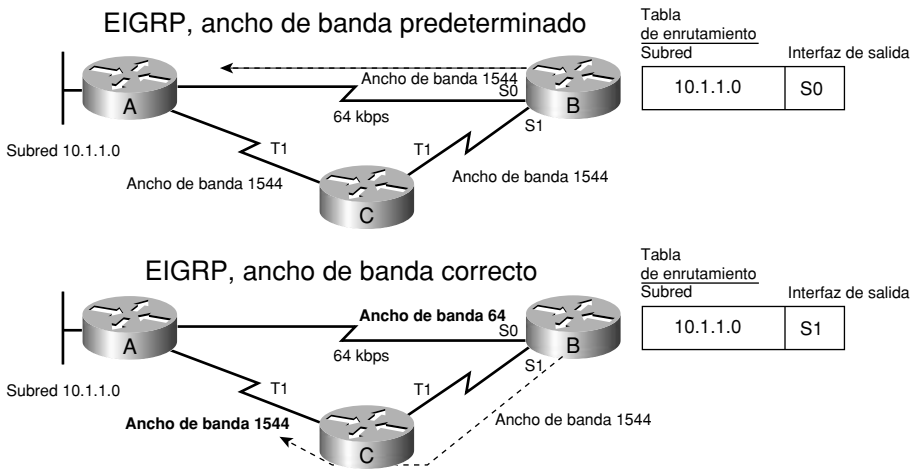


Figura 10.3. Efecto del ancho de banda sobre el cálculo de métricas de EIGRP.

la subred 10.1.1.0/24 en los dos casos. En la parte superior de la figura todas las interfaces serie utilizan valores predeterminados, aunque el enlace serie superior es de sólo 64 kbps. La figura inferior muestra los resultados cuando se modifica el comando bandwidth del enlace lento para reflejar su velocidad correcta (lenta).

Convergencia de EIGRP

Uno de los problemas más difíciles de cualquier protocolo de enrutamiento dinámico es evitar los bucles. Los protocolos por vector de distancia evitan este problema mediante toda una gama de herramientas, algunas de las cuales crean una gran parte de los tiempos de convergencia que duran minutos cuando falla un enlace. Los protocolos por estado del enlace evitan el problema haciendo que cada router mantenga una topología completa de la red, de tal manera que mediante la ejecución de un modelo matemático complejo el router puede evitar todos los bucles.

EIGRP evita los bucles manteniendo una información topológica básica, pero evita gastar demasiada CPU y demasiada memoria, haciendo que la información sea reducida. Cuando un router aprende múltiples rutas hacia una misma subred, pone la mejor ruta en la tabla de enrutamiento IP. EIGRP retiene cierta información topológica por la misma razón que OSPF, para que pueda converger muy rápidamente y utilizar una ruta nueva sin causar un bucle. En esencia, EIGRP mantiene un registro de cada posible router de siguiente salto, pero no tiene información sobre la topología más allá de los routers de siguiente salto. Esta información topológica más escasa no requiere el sofisticado algoritmo SPF, y da lugar a una convergencia rápida y a menos sobrecarga, sin bucles.

El proceso de convergencia EIGRP utiliza una de entre dos ramificaciones en su lógica, basándose en si la ruta que ha fallado posee o no una ruta que sea un **sucesor factible**. Si exis-

te una ruta sucesora factible, el router puede emplear inmediatamente esa ruta. En caso contrario, el router tiene que emplear un proceso de **consulta y respuesta** para buscar una ruta alternativa libre de bucles. Ambos procesos dan lugar a una convergencia rápida, normalmente de menos de 10 segundos, pero el proceso de pregunta y respuesta tarda un poquito más.

Sucesores y sucesores factibles en EIGRP

EIGRP calcula la métrica de cada ruta para alcanzar cada subred. Para una subred en particular, la ruta que tiene la mejor métrica se denomina sucesora, y el router rellena la tabla de enrutamiento IP con esta ruta. (La métrica de esta ruta se denomina distancia factible, como se indicaba anteriormente.)

De las otras rutas que llegan a la misma subred (rutas cuyas métricas eran más largas que la FD de la ruta), EIGRP necesita determinar cuál se puede utilizar inmediatamente si falla la que sea mejor en este momento, sin dar lugar a un bucle de enrutamiento. EIGRP ejecuta un algoritmo sencillo para identificar las rutas que se podrían utilizar, y mantiene estas rutas de respaldo libres de bucles en su base de datos topológica, para usarlas si falla la que actualmente es la mejor ruta. Estas rutas alternativas, que se pueden utilizar inmediatamente, reciben el nombre de **sucesoras factibles**, porque se pueden utilizar con certeza cuando falla la ruta sucesora. El router determina si una ruta es sucesora factible basándose en la siguiente condición de viabilidad:

> Si la RD de una ruta no sucesora es mejor que la FD, entonces esa ruta es una sucesora factible.

Aunque es técnicamente correcta, esta definición resulta mucho más comprensible mediante el ejemplo que se muestra en la Figura 10.4. La figura ilustra la forma en que EIGRP determina qué rutas son sucesoras factibles para la Subred 1. En la figura, el Router E aprende tres rutas hasta la Subred 1, pasando por los routers B, C y D. Después de calcular la métrica de cada ruta, basándose en la información de ancho de banda y de retardo recibida en la actualización de enrutamiento y en las correspondientes interfaces salientes de E, el Router E determina que la ruta que pasa por el Router D tiene la métrica más baja, así que el Router E añade esa ruta a su tabla de enrutamiento, según se muestra. La FD es la métrica calculada para esta ruta, que tiene el valor 14000 en este caso.

EIGRP decide si una ruta puede ser sucesora factible cuando la distancia informada para esa ruta (la métrica, tal como se ha calculado para ese vecino) es menor que la mejor de sus propias métricas calculadas (la FD). Cuando ese vecino tiene una métrica inferior para su ruta hasta la subred en cuestión, se dice que esa ruta satisface la **condición de viabilidad**. Por ejemplo, el Router E calcula una métrica (FD) de 14000 para su mejor ruta (que pasa por el Router D). La métrica calculada para el Router C (su distancia informada para esta ruta) es menor que 14000 (vale 13000). Como resultado, E sabe que la mejor ruta de C para esta subred no puede pasar por E, así que el Router E piensa que podría empezar a utilizar la ruta que pasa por C sin causar un bucle. Como resultado, el Router E añade una ruta que pasa por C a la tabla de topología como ruta sucesora factible. A la inversa, la distancia informada del Router B es 15000, que es mayor que la FD del Router E (14000), así que el Router E no considera que la ruta que pasa por B sea un sucesor factible.

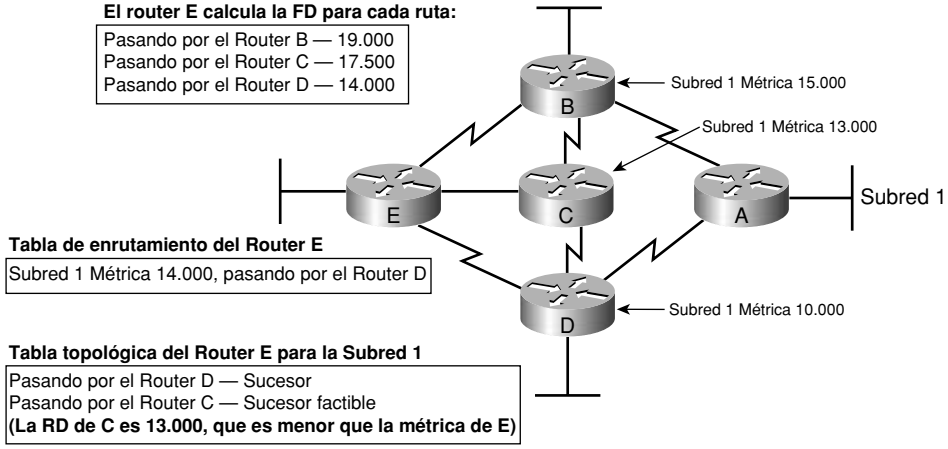


Figura 10.4. Sucesores y sucesores factibles con EIGRP.

Si la ruta que va a la Subred 1 a través del Router D falla, entonces el Router E puede poner inmediatamente la ruta que pasa por C en la tabla de enrutamiento sin temor de crear un bucle. En este caso, la convergencia se produce de forma casi instantánea.

El proceso de consulta y respuesta

Cuando falla una ruta y no tiene sucesora factible, EIGRP utiliza un algoritmo distribuido denominado **Algoritmo de actualización difuso** *(Diffusing Update Algorithm,* DUAL). DUAL envía preguntas en busca de una ruta libre de bucles a la subred en cuestión. Cuando se halla la nueva ruta, DUAL la añade a la tabla de enrutamiento.

El proceso DUAL de EIGRP se limita a utilizar mensajes para confirmar que existe una ruta, y que no va a crear un bucle, antes de optar por sustituir una ruta fallida por otra ruta alternativa. Por ejemplo, en la Figura 10.4, imagine que falla tanto el Router C como el D. El Router E no dispone de una ruta sucesora factible para la subred 1, pero hay una ruta que está obviamente disponible y que pasa por el Router B. Para utilizar esa ruta, el Router E envía mensajes de **consulta** EIGRP a sus vecinos operativos (en este caso, al Router B). La ruta del Router B hacia la subred 1 sigue funcionando perfectamente, así que el Router B contesta al Router E con un mensaje de **respuesta** EIGRP, indicando simplemente los detalles de la ruta operativa que va hasta la subred 1 y confirmando que sigue en estado utilizable. Entonces el Router E puede añadir una ruta nueva hacia la subred 1 a su tabla de enrutamiento, sin temor de que se produzca un bucle.

La sustitución de una ruta fallida por un sucesor viable requiere una cantidad de tiempo muy pequeña, normalmente menos de uno o dos segundos. Cuando se requieren preguntas y respuestas, la convergencia puede requerir algo más de tiempo, pero en la mayoría de las redes la convergencia se logra en menos de diez segundos.

Resumen de EIGRP y comparaciones con OSPF

EIGRP es un IGP popular por muchas razones. Funciona bien, y converge rápidamente al mismo tiempo que evita los bucles como efecto secundario de sus algoritmos híbridos equilibrados/por vector de distancia avanzados subyacentes. No requiere mucha configuración ni mucha planificación, ni siquiera cuando se amplía para dar soporte a redes más extensas.

EIGRP también tiene otra ventaja que no es tan importante en la actualidad como era en el pasado: admite los protocolos IPX de Novell y los protocolos de capa 3 AppleTalk de Apple. Los Routers pueden ejecutar EIGRP para aprender rutas IP, rutas IPX y rutas AppleTalk, manteniendo unas maravillosas características de rendimiento. Sin embargo, al igual que muchos otros protocolos de capa 3, IP ha sustituido en la mayoría de los casos a IPX y a AppleTalk, haciendo que el soporte de estos protocolos de capa 3 sea tan sólo una pequeña ventaja.

La Tabla 10.2 resume varias características importantes de EIGRP en comparación con OSPF.

Tabla 10.2. Características de EIGRP en comparación con OSPF

Tema clave

Característica	EIGRP	OSPF
Converge rápidamente	Sí	Sí
Prevención de bucles incorporada	Sí	Sí
Envía actualizaciones de enrutamiento parciales, notificando sólo la información nueva o modificada	Sí	Sí
No tiene clase; por tanto, admite los resúmenes manuales y VLSM	Sí	Sí
Admite los resúmenes manuales en cualquier router	Sí	No
Envía información de enrutamiento empleando multidifusión IP en las LANs	Sí	Sí
Utiliza el concepto de router designado en una LAN	No	Sí
Ofrece un diseño de red flexible, sin necesidad de crear áreas	Sí	No
Admite el equilibrado de la carga tanto para métricas iguales como para métricas desiguales	Sí	No
Métrica robusta, basada en ancho de banda y retardo	Sí	No
Puede publicar rutas IP, IPX y AppleTalk	Sí	No
Estándar público	No	Sí

Configuración y verificación de EIGRP

La configuración básica de EIGRP se parece mucho a la configuración de RIP y de OSPF. El comando router eigrp activa EIGRP y pone al usuario en el modo de configuración de EIGRP, en el cual se pueden configurar uno o más comandos network. Para cada interfaz que se especifique en un comando network, EIGRP intentará descubrir vecinos en esa interfaz, y EIGRP publicará la existencia de la subred conectada a la interfaz.

Esta sección examina la configuración de EIGRP, incluyendo varias características opcionales. También explica el significado del resultado de muchos comandos show para ayudar a conectar la teoría que se trata en la primera parte de este capítulo con la realidad de la implementación de EIGRP en el IOS. La siguiente lista de comprobación de la configuración esboza las principales tareas de configuración que se tratan en este capítulo:

- **Paso 1** Entrar en el modo de configuración EIGRP, y definir el ASN de EIGRP empleando el comando global router eigrp *número-as*.
- **Paso 2** Configurar uno o más subcomandos de router network *dirección-IP* [*máscara-wildcard*]. Esto activa EIGRP en las interfaces que se indiquen y da lugar a que EIGRP publique la existencia de de la subred conectada.
- **Paso 3** (Opcional) Modificar los temporizadores Hello y de espera de la interfaz, empleando los subcomandos de interfaz ip hello-interval eigrp *asn tiempo* y ip hold-time eigrp *asn tiempo*.
- **Paso 4** (Opcional) Modificar los cálculos de métrica, efectuando un ajuste fino del ancho de banda y del retardo mediante los subcomandos de interfaz bandwidth *valor* y delay *valor*.
- **Paso 5** (Opcional) Configurar la autenticación EIGRP.
- **Paso 6** (Opcional) Configurar el soporte para múltiples rutas de igual coste, empleando los subcomandos de router maximum-paths *número* y variance *multiplicador*.

Configuración básica de EIGRP

El Ejemplo 10.1 muestra para la Figura 10.5 un caso de configuración de EIGRP, junto con comandos show, en Albuquerque. La configuración EIGRP necesaria en Yosemite y Seville coincide exactamente con las dos últimas líneas de la configuración de Albuquerque.

Para la configuración EIGRP, los tres routers tienen que utilizar el mismo número de AS en el comando router eigrp. Por ejemplo, en este caso todos ellos utilizan router eigrp 1. El número en sí no importa realmente, siempre y cuando sea el mismo en los tres routers. (El rango de números de AS válidos va desde 1 hasta 65535, al igual que el rango de ID de proceso válidos en el comando router ospf.) El comando network 10.0.0.0 habilita EIGRP en todas aquellas interfaces cuyas direcciones IP se encuentren en la red 10.0.0.0, lo cual incluye las tres interfaces de Albuquerque. Empleando dos sentencias de configuración EIGRP idénticas en los otros dos routers, EIGRP queda habilitado también en las tres interfaces de esos routers, porque esas interfaces también se encuentran en la red 10.0.0.0.

Ejemplo 10.1. Ejemplo de configuración de un router con EIGRP activado.

```
router eigrp 1
 network 10.0.0.0
Albuquerque#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 6 subnets
D       10.1.3.0 [90/2172416] via 10.1.6.3, 00:00:43, Serial0/1
D       10.1.2.0 [90/2172416] via 10.1.4.2, 00:00:43, Serial0/0
C       10.1.1.0 is directly connected, FastEthernet0/0
C       10.1.6.0 is directly connected, Serial0/1
D       10.1.5.0 [90/2681856] via 10.1.6.3, 00:00:45, Serial0/1
                 [90/2681856] via 10.1.4.2, 00:00:45, Serial0/0
C       10.1.4.0 is directly connected, Serial0/0

Albuquerque#show ip route eigrp
     10.0.0.0/24 is subnetted, 6 subnets
D       10.1.3.0 [90/2172416] via 10.1.6.3, 00:00:47, Serial0/1
D       10.1.2.0 [90/2172416] via 10.1.4.2, 00:00:47, Serial0/0
D       10.1.5.0 [90/2681856] via 10.1.6.3, 00:00:49, Serial0/1
                 [90/2681856] via 10.1.4.2, 00:00:49, Serial0/0

Albuquerque#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H    Address       Interface    Hold Uptime     SRTT     RTO  ipQ    Seq Type
                                (sec)           (ms)      ipipipCnt  Num
0    10.1.4.2      Se0/0        11 00:00:54     32       200  ip0    4
1    10.1.6.3      Se0/1        12 00:10:36     20       200  ip0    24

Albuquerque#show ip eigrp interfaces
IP-EIGRP interfaces for process 1

                     Xmit Queue    Mean    Pacing Time    Multicast      Pending
Interface    Peers   Un/Reliable   SRTT    Un/Reliable    Flow Timer     Routes
Fa0/0          0        0/0          0       0/10            0             0
Se0/0          1        0/0         32       0/15           50             0
Se0/1          1        0/0         20       0/15           95             0
Albuquerque#show ip eigrp topology summary
IP-EIGRP Topology Table for AS(1)/ID(10.1.6.1)
Head serial 1, next serial 9
6 routes, 0 pending replies, 0 dummies
IP-EIGRP(0) enabled on 3 interfaces, 2 neighbors present on 2 interfaces
Quiescent interfaces: Se0/1/0 Se0/0/1
```

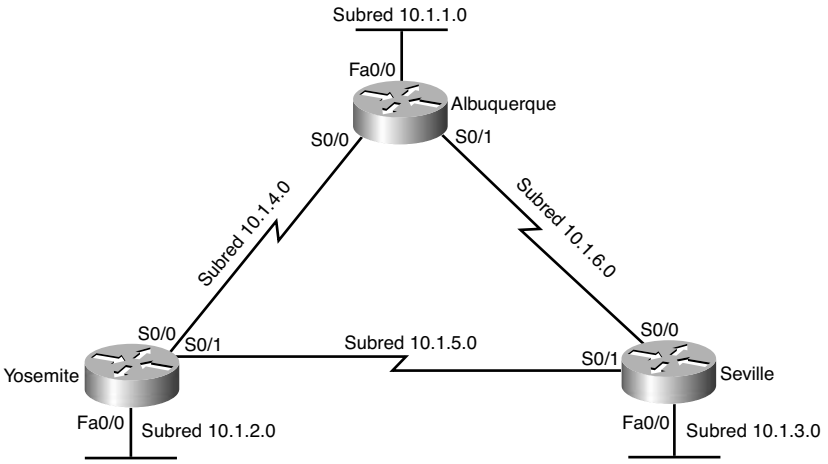


Figura 10.5. Ejemplo de red empleada en la mayoría de los ejemplos de EIGRP.

Los comandos show ip route y show ip route eigrp muestran ambos las rutas aprendidas con EIGRP con una "D" a su lado. La "D" significa EIGRP. La letra E ya se estaba utilizando para el Protocolo de gateway exterior (*Exterior Gateway Protocol*, EGP) cuando Cisco creó EIGRP, así que Cisco seleccionó la letra más parecida que no se estaba utilizando, la D, para denotar las rutas aprendidas mediante EIGRP.

Se puede obtener información relativa a los vecinos EIGRP empleando el comando show ip eigrp neighbors, e información relativa al número de vecinos activos (que se denominan pares en la salida del comando) mediante el comando show ip eigrp interfaces, como puede verse en la última parte del ejemplo. Estos comandos también permiten hacerse una idea de los procesos subyacentes de EIGRP, como el uso de RTP para disponer de unas transmisiones fiables. Por ejemplo, el comando show ip eigrp neighbors muestra una columna titulada "Q Cnt" (*Queue Count*), que indica el número de paquetes en espera para ser enviados a un vecino, o bien los paquetes que se han enviado pero para los cuales no se obtenido un acuse de recibo. El comando show ip eigrp interfaces muestra una información parecida en la columna "Xmit Queue Un/Reliable" (cola de transmisión fiable/no fiable) que separa las estadísticas para los mensajes que se envían mediante RTP (fiable) o sin este protocolo (no fiable).

Por último, la parte final del ejemplo muestra el RID de Albuquerque. EIGRP asigna su RID exactamente igual que OSPF, basándose en el valor configurado, o en la dirección IP más alta de una interfaz *loopback* que esté en el estado *up/up*, por este orden de prioridades. La única diferencia respecto a OSPF es que el RID de EIGRP se configura mediante el subcomando de router eigrp router-id *valor*.

El comando EIGRP network se puede configurar sin una máscara *wildcard*, como se muestra en el Ejemplo 10.1. Sin dicha máscara, el comando network tiene que utilizar una red con clase como único parámetro, y todas las interfaces de la red con clase quedan seleccionadas. El Ejemplo 10.2 muestra una configuración alternativa que hace uso de un

comando network dotado de una dirección y de una máscara *wildcard*. En este caso, el comando selecciona una dirección IP de interfaz que sería seleccionada si la dirección y la máscara del comando network formaran parte de alguna ACL. El ejemplo muestra tres comandos network en Albuquerque, cada uno de los cuales coincide con una de las interfaces.

Ejemplo 10.2. Utilización de máscaras *wildcard* en la configuración de EIGRP.

```
Albuquerque#router eigrp 1
Albuquerque(config-router)#network 10.1.1.0 0.0.0.255
Albuquerque(config-router)#network 10.1.4.0 0.0.0.255
Albuquerque(config-router)#network 10.1.6.0 0.0.0.255
```

Métricas, sucesores y sucesores factibles en EIGRP

Según se ha definido anteriormente en este capítulo, una ruta sucesora de EIGRP es una ruta que tiene la mejor métrica para llegar a una subred, y una ruta sucesora factible (FS) es una ruta que se podría utilizar si fallase la ruta sucesora. Esta sección examina la forma de ver las rutas sucesoras y FS con EIGRP, junto con las métricas calculadas. Con este objeto, el Ejemplo 10.3 muestra la mejor de las rutas de Albuquerque para llegar a la subred 10.1.3.0/24, tanto en la tabla de enrutamiento como ruta sucesora en la tabla topológica de EIGRP. También se muestran las dos rutas sucesoras de igual métrica para la subred 10.1.5.0/24, y estas dos rutas sucesoras están resaltadas en la tabla topológica de EIGRP. Algunas de las explicaciones se muestran en el ejemplo, y las explicaciones más extensas siguen al ejemplo.

Los comentarios del ejemplo explican las cuestiones fundamentales, la mayoría de las cuales son relativamente sencillas. Sin embargo, si se examina más detalladamente el comando show ip eigrp topology, se hace uno a la idea de más cosas. En primer lugar, considere la tabla topológica de EIGRP que muestra el número de rutas sucesoras. La entrada para 10.1.3.0/24 dice que hay un sucesor, así que la tabla de enrutamiento IP muestra una ruta aprendida con EIGRP que lleva a la subred 10.1.3.0/24. Sin embargo, la entrada de la tabla topológica EIGRP correspondiente a la subred 10.1.5.0/24 dice que hay dos sucesores, así que la tabla de enrutamiento IP muestra dos rutas aprendidas por EIGRP que llevan a esa subred.

Consideremos ahora los números que van entre corchetes junto a la entrada para 10.1.3.0/24 en la tabla topológica de EIGRP. El primer número es la métrica calculada por Albuquerque para cada ruta. El segundo número es la RD, esto es, la métrica tal como ha sido calculada en el router vecino 10.1.6.3 (Seville) y notificada a Alburquerque. Como estos routers tienen el valor predeterminado para la configuración de ancho de banda y de retardo, los valores de la métrica coinciden con los cálculos dados como ejemplo en la sección "Cálculo de las mejores rutas para la tabla de enrutamiento", anteriormente en este capítulo.

Ejemplo 10.3. Uso de máscaras *wildcard* con la configuración EIGRP, y examen de sucesores factibles.

```
! Obsérvese más abajo que hay una sola ruta para la subred 10.1.3.0, y
! que hay dos rutas de igual métrica para 10.1.5.0.
Albuquerque#show ip route
Codes:  C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 6 subnets
D        10.1.3.0 [90/2172416] via 10.1.6.3, 00:00:57, Serial0/1
D        10.1.2.0 [90/2172416] via 10.1.4.2, 00:00:57, Serial0/0
C        10.1.1.0 is directly connected, Ethernet0/0
C        10.1.6.0 is directly connected, Serial0/1
D        10.1.5.0 [90/2681856] via 10.1.4.2, 00:00:57, Serial0/0
                  [90/2681856] via 10.1.6.3, 00:00:57, Serial0/1
C        10.1.4.0 is directly connected, Serial0/0
! A continuación, la tabla topológica de EIGRP muestra un sucesor para
! la ruta hacia 10.1.3.0, y dos sucesores para 10.1.5.0, confirmando
! de nuevo que EIGRP instala rutas sucesoras (no rutas sucesoras factibles)
! en la tabla de enrutamiento IP.
Albuquerque#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(10.1.6.1)

Codes:  P - Passive, A - Active, U - Update, Q - Query, R - Reply,
        r - reply Status, s - sia Status

P 10.1.3.0/24, 1 successors, FD is 2172416
        via 10.1.6.3 (2172416/28160), Serial0/1
P 10.1.2.0/24, 1 successors, FD is 2172416
        via 10.1.4.2 (2172416/28160), Serial0/0
P 10.1.1.0/24, 1 successors, FD is 281600
        via Connected, Ethernet0/0
P 10.1.6.0/24, 1 successors, FD is 2169856
        via Connected, Serial0/1
P 10.1.5.0/24, 2 successors, FD is 2681856
        via 10.1.4.2 (2681856/2169856), Serial0/0
        via 10.1.6.3 (2681856/2169856), Serial0/1
P 10.1.4.0/24, 1 successors, FD is 2169856
        via Connected, Serial0/0
```

Creación y visualización de una ruta sucesora factible

Como se han empleado todas las configuraciones predeterminadas, ninguna de las rutas de Albuquerque satisface la condición de viabilidad, según la cual la RD de una ruta alternativa es menor o igual que la FD (la métrica de la mejor ruta). En el Ejemplo 10.4 se modifica el ancho de banda de una de las interfaces de Yosemite, reduciendo la FD de Yosemite para llegar a la subred 10.1.3.0/24. A su vez, la RD de Yosemite para esta misma ruta, según se le notifica a Albuquerque, se verá reducida, y llegará a satisfacer la condición de viabilidad, así que ahora Albuquerque dispondrá de una ruta FS.

Ejemplo 10.4. Creación de una ruta sucesora factible en Albuquerque.

```
! A continuación se cambia el ancho de banda del enlace de Yosemite
! a Seville (interfaz S0/1 de Yosemite), pasando de 1544
! a 2000, lo cual reduce la métrica de Yosemite para la subred 10.1.3.0.
Yosemite(config)#interface S0/1
Yosemite(config-if)#bandwidth 2000
```

```
! De vuelta a Albuquerque
! A continuación, la tabla topológica de EIGRP muestra una única ruta
! sucesora para 10.1.3.0, pero se muestran dos entradas; la nueva entrada
! es una ruta sucesora factible. La nueva entrada muestra una ruta hacia
! 10.1.3.0 que pasa por 10.1.4.2 (que es Yosemite).
Albuquerque#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(10.1.6.1)
Codes:  P - Passive, A - Active, U - Update, Q - Query, R - Reply,
        r - reply Status, s - sia Status

P 10.1.3.0/24, 1 successors, FD is 2172416
         via 10.1.6.3 (2172416/28160), Serial0/1
         via 10.1.4.2 (2684416/1794560), Serial0/0
! Se omiten las líneas restantes por brevedad
! Volvemos a Yosemite
Yosemite#show ip route eigrp
      10.0.0.0/24 is subnetted, 5 subnets
D        10.1.3.0 [90/1794560] via 10.1.5.3, 00:40:14, Serial0/1
D        10.1.1.0 [90/2195456] via 10.1.4.1, 00:42:19, Serial0/0
```

Para ver la ruta sucesora factible, y por qué es una sucesora factible, considérense los dos números que se muestran entre paréntesis en la segunda línea resaltada del comando show ip eigrp topology ejecutado en Albuquerque. La primera es la métrica calculada en Albuquerque para la ruta, y el segundo número es la RD del vecino. De las dos rutas posibles (una que pasa por 10.1.6.3 [Seville] y otra que pasa por 10.1.4.2 [Yosemite]) la que pasa por Seville es la que tiene una métrica menor (2.172.416), lo cual la hace la ruta sucesora, y también hace que la FD sea 2.172.416. Albuquerque pone esta ruta en la tabla de enrutamiento IP. Sin embargo, obsérvese la RD de la segunda de estas dos rutas (la ruta que pasa por Yosemite), y cuyo valor RD es de 1.794.560. La condición de viabilidad consiste en que la RD de la ruta sea menor que la métrica calculada de la mejor ruta (su FD) para la misma

subred de destino. Por tanto, la ruta que pasa por Yosemite satisface esta condición, haciendo que sea una ruta sucesora factible. Los puntos siguientes resumen la información clave relativa a las rutas sucesoras y sucesoras factibles en este ejemplo:

- La ruta a 10.1.3.0 pasando por 10.1.6.3 (Seville) es la ruta sucesora, porque la métrica calculada (2.172.416), que se muestra como el primero de los dos números que van entre paréntesis, es la mejor métrica calculada.
- La ruta a 10.1.3.0 pasando por 10.1.4.2 (Yosemite) es una ruta sucesora factible, porque la distancia informada del vecino (1.794.560, que se muestra como segundo número entre paréntesis) es menor que la FD de Alburquerque.
- Aunque tanto la ruta sucesora como la ruta sucesora factible están en la tabla topológica EIGRP, sólo la ruta sucesora se añade a la tabla de enrutamiento IP.

Nota

El comando show ip eigrp topology muestra solamente las rutas sucesoras y sucesoras factibles. Para ver las otras rutas, utilice el comando show ip eigrp topology all-links.

Convergencia empleando la ruta sucesora factible

Una de las ventajas de EIGRP es que converge muy rápidamente. El Ejemplo 10.5 muestra uno de estos casos, empleando mensajes debug para documentar el proceso. Algunos de los mensajes debug podrían no tener mucho sentido, pero ciertamente este ejemplo pone de manifiesto unos cuantos mensajes debug comprensibles e interesantes.

Para este ejemplo se ha desactivado el enlace que hay entre Albuquerque y Seville, pero esto no se muestra en el ejemplo. Los mensajes debug de Albuquerque muestran comentarios relativos a la lógica de EIGRP al cambiar de la ruta original hacia 10.1.3.0/24 a una nueva ruta que pasa por Yosemite. Preste especial atención a las indicaciones de tiempos, que muestran que todo el proceso de convergencia requiere menos de 1 segundo.

Ejemplo 10.5. Mensajes de depuración generados durante la convergencia a una ruta sucesora factible para la subred 10.1.3.0/24.

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! En lo que sigue, debug eigrp fsm está activado, y después se desactivará
! el enlace de Seville a Albuquerque (la interfaz S0/0 de Seville)
! pero esto no se muestra en el texto del ejemplo. Se han omitido algunos
! mensajes de depuración para mejorar la legibilidad.
Albuquerque#debug eigrp fsm
EIGRP FSM Events/Actions debugging is on
Albuquerque#
*Mar  1 02:35:31.836: %LINK-3-UPDOWN: Interface Serial0/1, changed state to down
*Mar  1 02:35:31.848: DUAL: rcvupdate: 10.1.6.0/24 via Connected metric 42949672
95/4294967295
```

(continúa)

Ejemplo 10.5. Mensajes de depuración generados durante la convergencia a una ruta sucesora factible para la subred 10.1.3.0/24 *(continuación).*

```
*Mar  1 02:35:31.848: DUAL: Find FS for dest 10.1.6.0/24. FD is 2169856, RD is 2
169856
*Mar  1 02:35:31.848: DUAL: 0.0.0.0 metric 4294967295/4294967295 not found D
min is 4294967295
*Mar  1 02:35:31.848: DUAL: Peer total/stub 2/0 template/full-stub 2/0
*Mar  1 02:35:31.848: DUAL: Dest 10.1.6.0/24 entering active state.
*Mar  1 02:35:31.852: DUAL: Set reply-status table. Count is 2.
*Mar  1 02:35:31.852: DUAL: Not doing split horizon
!
! A continuación, Albuquerque percibe que el vecino 10.1.6.3 (Seville)
! está desactivado, así que Albuquerque puede reaccionar.
!
*Mar  1 02:35:31.852: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.6.3
  (Serial0/1) is down: interface down
!
! Los dos mensajes resaltados siguientes implican que la vieja ruta hacia
! 10.1.3.0 se ha eliminado, y que la nueva ruta sucesora (que antes era la
! ruta sucesora factible) se añade a la "RT" (tabla de enrutamiento).
!
*Mar  1 02:35:31.852: DUAL: Destination 10.1.3.0/24
*Mar  1 02:35:31.852: DUAL: Find FS for dest 10.1.3.0/24. FD is 2172416,
  RD is 2172416
*Mar  1 02:35:31.856: DUAL: 10.1.6.3 metric 4294967295/4294967295
*Mar  1 02:35:31.856: DUAL: 10.1.4.2 metric 2684416/1794560 found Dmin is 2684416
!
! Los dos siguientes mensajes resaltados indican que se ha
! eliminado la ruta vieja y que la nueva a través de Yosemite
! se ha añadido a la "RT" (tabla de enrutamiento).
!
*Mar  1 02:35:31.856: DUAL: Removing dest 10.1.3.0/24, nexthop 10.1.6.3
*Mar  1 02:35:31.856: DUAL: RT installed 10.1.3.0/24 via 10.1.4.2
*Mar  1 02:35:31.856: DUAL: Send update about 10.1.3.0/24. Reason: metric chg
*Mar  1 02:35:31.860: DUAL: Send update about 10.1.3.0/24. Reason: new if
```

Autenticación en EIGRP

EIGRP admite un solo tipo de autenticación: MD5. La configuración de una autenticación MD5 requiere varios pasos:

Paso 1 Crear una cadena de claves (de autenticación):

- **a.** Crear la cadena y darle un nombre mediante el comando global `key chain` *nombre* (además, esto pone al usuario en el modo de configuración de cadenas de claves).
- **b.** Crear uno o más números de clave empleando el comando `key` *número* en el modo de configuración de cadenas de claves.

c. Definir el valor de la clave de autenticación empleando el comando key-string *valor* en el modo de configuración de cadenas de claves.

d. (Opcional) Definir la duración (periodo de validez) tanto para enviar como para aceptar esta clave concreta.

Paso 2 Activar la autenticación EIGRP MD5 en una interfaz, para un cierto ASN de EIGRP, empleando el subcomando de interfaz ip authentication mode eigrp *asn* md5.

Paso 3 Referirse a la cadena de claves correcta que hay que emplear en una interfaz, empleando el subcomando de interfaz ip authentication key-chain eigrp *asn nombre-de-cadena*.

La configuración del Paso 1 es bastante minuciosa, pero los Pasos 2 y 3 son relativamente sencillos. En esencia, el IOS configura los valores de las claves por separado, y después requiere un subcomando de interfaz para referirse a los valores de las claves. Para admitir la posibilidad de disponer de múltiples claves, e incluso de múltiples conjuntos de claves, la configuración incluye el concepto de cadena de claves y de múltiples claves en cada cadena de claves.

El concepto de cadena de claves en el IOS se parece al de los llaveros y las llaves que se utilizan en la vida diaria. Casi todas las personas tienen al menos un llavero, que contiene las llaves que utilizan todos los días. Si uno tiene muchas llaves para el trabajo y para casa, quizá tenga dos llaveros para que sea más fácil encontrar la llave correcta. También se podría tener un llavero para llaves de uso poco frecuente, que estaría en algún cajón. De manera similar, el IOS permite configurar múltiples cadenas de claves para que se puedan usar distintas claves en distintas interfaces. Cada cadena de claves puede contener varias claves. Al tener múltiples claves en una misma cadena, se permite que los vecinos sigan funcionando mientras se cambian las claves. (Tal como sucede con las contraseñas y con las claves de autenticación, cambiar las claves ocasionalmente mejora la seguridad.) Para configurar estos detalles importantes, siga los Pasos 1A, 1B y 1C con objeto de crear la cadena de claves, crear una o más claves y asignar la clave de texto (la contraseña).

El último elemento opcional que se puede configurar para la autenticación EIGRP es la vida útil de cada clave. Si no se configura esto, la clave es válida para siempre. Sin embargo, si se configura, el router sólo utiliza la clave durante el periodo indicado. Esta característica permite que la cadena de claves incluya varias claves, cada una de ellas con duraciones distintas. Por ejemplo, se podrían definir 12 claves, una para cada mes del año. Entonces los routers utilizarían automáticamente la clave de número más bajo cuyo intervalo temporal fuera válido, cambiando las claves automáticamente cada mes en el ejemplo que se menciona. Esta característica permite a los ingenieros configurar las claves una sola vez y hacer que los routers utilicen claves nuevas ocasionalmente, mejorando de este modo la seguridad.

Para que pueda soportar el concepto de vida útil, el router tiene que conocer la fecha y la hora. Los routers pueden establecer la fecha y la hora mediante el comando EXEC clock set. Los routers también pueden utilizar el Protocolo de tiempo de red (*Network Time Protocol*, NTP), que permite a los routers sincronizar sus relojes a una misma hora.

La mejor manera de apreciar la configuración consiste en ver un ejemplo. El Ejemplo 10.6 muestra una configuración que hace uso de dos cadenas de claves. La cadena

Ejemplo 10.6. Autenticación en EIGRP.

```
! La cadena "carkeys" se utilizará en la interfaz Fa0/0 de R1. R1 utilizará
! la clave "fred" durante aproximadamente un mes,
! y después empezará a utilizar "wilma."
!
key chain carkeys
 key 1
 key-string fred
 accept-lifetime 08:00:00 Jan 11 2005 08:00:00 Feb 11 2005
 send-lifetime 08:00:00 Jan 11 2005 08:00:00 Feb 11 2005
 key 2
 key-string wilma
 accept-lifetime 08:00:00 Feb 10 2005 08:00:00 Mar 11 2005
 send-lifetime 08:00:00 Feb 10 2005 08:00:00 Mar 11 2005
! A continuación, la cadena "anothersetofkeys" define la clave
! que se utilizará en Fa0/1.
key chain anothersetofkeys
 key 1
 key-string barney
!
! A continuación, se muestran los subcomandos de interfaz de R1.
! En primer lugar, se hace alusión a la cadena de claves empleando
! el comando ip authentication key-chain, y el comando ip authentication
! mode eigrp hace que el router utilice un compendio MD5 de la cadena de claves.
interface FastEthernet0/0
 ip address 172.31.11.1 255.255.255.0
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 carkeys
!
! Ahora, R1 activa la autenticación EIGRP en la interfaz Fa0/1,
! empleando la otra cadena de claves.
interface FastEthernet0/1
 ip address 172.31.12.1 255.255.255.0
 ip authentication eigrp 1 md5
 ip authentication key-chain eigrp 1 anothersetofkeys
```

"fred" tiene dos claves, así que el router utilizará automáticamente claves nuevas con el paso del tiempo. También muestra el uso de las dos cadenas de claves en dos interfaces distintas.

Para que funcione la autenticación, los routers vecinos tienen que tener activada la autenticación MD5 de EIGRP, y las cadenas de claves que utilicen en ese momento deben coincidir. Obsérvese que no es preciso que coincidan los nombres de las cadenas de claves. Los problemas más comunes están relacionados con que no coincida la configuración de vida útil, o con que el reloj de alguno de los routers no tenga una hora correcta. Para las implementaciones del mundo real, NTP debería estar activado y en uso antes de limitar las claves a un determinado periodo de tiempo.

Para verificar que ha funcionado la autenticación, utilice el comando show ip eigrp neighbors. Si falla la autenticación, no se constituirá una relación de vecindad. Por otra parte, si en esa interfaz se ven rutas aprendidas de un vecino, esto demuestra que la autenticación ha funcionado. Pueden obtenerse más detalles del proceso de autenticación empleando el comando debug eigrp packets, especialmente si falla la autenticación.

Rutas máximas y varianza en EIGRP

Al igual que OSPF, EIGRP tiene la capacidad de poner múltiples rutas de igual métrica en la tabla de enrutamiento. EIGRP también admite cuatro de esas rutas de forma predeterminada para cada subred, y se puede configurar para admitir un máximo de 16 empleando el subcomando EIGRP maximum-paths *número*. Sin embargo, el cálculo de métricas de EIGRP suele impedir que las rutas competidoras tengan exactamente la misma métrica. La fórmula puede producir resultados similares, pero dado que los valores de las métricas pueden ser del orden de millones, el cálculo de una métrica de valor exactamente igual al de otra es estadísticamente improbable.

El IOS ofrece el concepto de varianza EIGRP para resolver este problema. La varianza permite considerar como iguales aquellas rutas cuyas métricas tengan valores relativamente próximos, lo cual hace posible añadir múltiples rutas de una misma subred con métricas desiguales a la tabla de enrutamiento.

El subcomando de router EIGRP variance *multiplicador* define un entero entre 1 y 128. Entonces el router multiplica la varianza por la FD de la ruta, que es la mejor métrica para alcanzar esa subred. Aquellas rutas FS cuya métrica sea menor que el producto de la varianza por la FD se consideran rutas iguales y se pueden poner en la tabla de enrutamiento, dependiendo del ajuste especificado mediante el comando maximum-paths.

Veamos un ejemplo de varianza para clarificar este concepto. Para que los números sean más obvios, la Tabla 10.3 muestra un ejemplo en el cual los valores de las métricas son pequeños. La tabla muestra las métricas de tres rutas para llegar a una misma subred, calculadas en el router R4. La tabla muestra también la RD de los routers vecinos, y la decisión de añadir rutas a la tabla de enrutamiento basada en distintas configuraciones de varianza.

Tabla 10.3. Ejemplo de rutas que se consideran iguales por efecto de la varianza.

Siguiente salto	Métrica	RD	¿Se añade a RT con varianza 1?	¿Se añade a RT con varianza 2?	¿Se añade a RT con varianza 3?
R1	50	30	Sí	Sí	Sí
R2	90	40	No	Sí	Sí
R3	120	60	No	No	No

Antes de considerar la varianza, obsérvese que en este caso la ruta que pasa por R1 es la ruta sucesora, porque es la que tiene la métrica más baja. Esto significa también que la

métrica de la ruta que pasa por R1, 50, es la FD. La ruta que pasa por R2 es una ruta FS porque su RD, de 40, es menor que la FD de 50. La ruta que pasa por R3 no es una ruta FS porque la RD de R3, que vale 60, es mayor que la FD, que vale 50.

Cuando la varianza tiene su valor predeterminado, que es de 1, las métricas tienen que ser exactamente iguales para considerarse iguales, así que sólo se añadirá la ruta sucesora a la tabla de enrutamiento. Si la varianza es 2, la FD (50) se multiplica por la varianza (2) y el producto es 100. La ruta que pasa por R2, cuya FD es 90, es menor que 100, así que R4 añade también la ruta que pasa por R2 a la tabla de enrutamiento. Entonces el router puede equilibrar la carga de tráfico enviándolo a través de estas dos rutas.

En el tercer caso, con una varianza de 3, el producto de la FD (50) por 3 produce un producto de 150, y las métricas calculadas para las tres rutas son menores que 150. Sin embargo, la ruta que pasa por R3 no es una ruta FS, así que no se puede añadir a la tabla de enrutamiento por miedo a crear un bucle de enrutamiento.

La lista siguiente resume los puntos clave de la varianza:

- La varianza se multiplica por la FD actual (la métrica de la mejor ruta para llegar a la subred).
- Aquellas rutas FS cuya métrica calculada sea menor o igual que el producto de la varianza por la FD se añaden a la tabla de enrutamiento IP, suponiendo que el ajuste de maximum-paths permita añadir más rutas.
- Aquellas rutas que no son sucesoras ni sucesoras factibles no se pueden añadir nunca a la tabla de enrutamiento IP, independientemente del ajuste que se haya especificado para la varianza.

En cuanto las rutas se han añadido a la tabla de enrutamiento, el router ofrece toda una gama de opciones para equilibrar la carga de tráfico que pasa por las rutas. El router puede equilibrar el tráfico proporcionalmente a las métricas, lo cual significa que las rutas que tienen métricas más bajas envían más paquetes. El router puede enviar todo el tráfico a través de la ruta con la métrica más baja, dejando las demás rutas de la tabla de enrutamiento para acelerar la convergencia si falla la mejor ruta. Sin embargo, los detalles del proceso de equilibrado de cargas requieren una discusión mucho más profunda de las interioridades del proceso de reenvío en el IOS, y ese tema va más allá de los límites de este libro.

Ajuste fino del cálculo de métricas en EIGRP

De manera predeterminada, EIGRP calcula una métrica entera que está basada en la métrica compuesta de ancho de banda y retardo. Se pueden cambiar ambos ajustes en cualquier interfaz, empleando los subcomandos de interfaz bandwidth *valor* y delay *valor*.

Cisco recomienda dar al ancho de banda de las interfaces un valor preciso, en lugar de configurar el ancho de banda con objeto de modificar el cálculo de la métrica de EIGRP. Aunque las interfaces LAN toman como valor predeterminado unos ajustes precisos del ancho de banda, los enlaces serie de los routers deberían configurarse mediante el comando bandwidth *velocidad*, indicando el valor de la velocidad en kbps, y haciendo que coincida con la velocidad real de la interfaz.

Como la configuración del retardo de la interfaz influye sobre menos características, Cisco recomienda que si se quiere hacer un ajuste fino de la métrica EIGRP se modifique el ajuste del retardo. Para modificar la configuración del retardo de una interfaz, utilice el comando delay *valor*, donde el valor es el ajuste del retardo, empleando una unidad poco frecuente: las decenas de microsegundos. Curiosamente, la fórmula de la métrica EIGRP también utiliza como unidad las decenas de microsegundos; sin embargo, el comando show muestra el retardo empleando los microsegundos como unidades. El Ejemplo 10.7 muestra un ejemplo, con los detalles siguientes:

1. La interfaz Fa0/0 del router tiene un ajuste predeterminado del retardo igual a 100 microsegundos (μs).
2. En la interfaz se configura el comando delay 123, lo cual significa 123 decenas de μs.
3. Ahora, el comando show interfaces fa0/0 muestra un retardo de 1230 μs.

Ejemplo 10.7. Configuración del retardo en una interfaz.

```
Yosemite#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 0013.197b.5026 (bia 0013.197b.5026)
  Internet address is 10.1.2.252/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
! Líneas omitidas por brevedad

Yosemite#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yosemite(config)#interface fa0/0
Yosemite(config-if)#delay 123
Yosemite(config-if)#^Z

Yosemite#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 0013.197b.5026 (bia 0013.197b.5026)
  Internet address is 10.1.2.252/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1230 usec,
! Líneas omitidas por brevedad
```

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 10.4 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 10.4. Temas clave del Capítulo 10.

Tema clave	Descripción	Número de página
Lista	Razones que impiden que los routers EIGRP se hagan vecinos.	381
Figura 10.1	Representa el proceso normal de descubrimiento de vecinos, las actualizaciones de enrutamiento completas, los Hellos continuos y las actualizaciones parciales.	382
Lista	Definiciones de distancia factible y distancia informada.	385
Figura 10.4	Ejemplo de la forma en que los routers determinan qué rutas son sucesores factibles.	388
Tabla 10.2	Comparación de las características de EIGRP y de OSPF.	389
Lista	Lista de comprobación para la configuración de EIGRP.	390
Lista	Puntos clave relativos a la forma de obtener una ruta sucesora factible a partir del resultado del comando show.	396
Lista	Lista de comprobación para configurar la autenticación MD5 en EIGRP.	397-398
Lista	Puntos clave respecto a la varianza EIGRP.	401

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD), o por lo menos de la sección de este capítulo, y complete de memoria las tablas y listas. El Apéndice K, "Respuestas a los ejercicios de memorización". también disponible en el DVD, incluye las tablas y las listas ya completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe las respuestas en el glosario:

Actualización completa, actualización parcial, condición de viabilidad, distancia factible, distancia informada, sucesor, sucesor factible.

Referencias de comandos

Aunque no necesariamente debe memorizar la información de las tablas de esta sección, ésta incluye una referencia de los comandos de configuración y EXEC utilizados en este capítulo. En la práctica, debería memorizar los comandos como un efecto colateral de leer el capítulo y hacer todas las actividades de esta sección de preparación del examen. Para verificar si ha memorizado los comandos como un efecto secundario de sus otros estudios, cubra el lado izquierdo de la tabla con un trozo de papel, lea las descripciones del lado derecho, y compruebe si recuerda el comando.

Tabla 10.5. Comandos de configuración del Capítulo 10.

Comando	Descripción
router eigrp *sistema-autónomo*	Comando global para llevar al usuario al modo de configuración EIGRP para el ASN especificado.
network *número-de-red* [*máscara-wildcard*]	Subcomando EIGRP que denota todas las interfaces de una red con clase, o un subconjunto de las interfaces, basándose en una máscara *wildcard* de tipo similar al de una ACL, para habilitar EIGRP en esas interfaces.
maximum-paths *número-de-rutas*	Subcomando de router que define el número máximo de rutas de igual coste que se pueden añadir a la tabla de enrutamiento.
variance *multiplicador*	Subcomando de router que define un multiplicador EIGRP que sirve para determinar si la métrica de una ruta sucesora factible es suficientemente parecida a la métrica de la sucesora para considerarla igual.
bandwidth *ancho-de-banda*	Subcomando de interfaz que establece directamente el ancho de banda (kbps).
delay *valor-de-retardo*	Subcomando de interfaz para establecer el valor de retardo de la interfaz, empleando como unidades las decenas de microsegundos.

(continúa)

Tabla 10.5. Comandos de configuración del Capítulo 10 *(continuación).*

Comando	Descripción
ip hello-interval eigrp *número-as valor-temporizador*	Subcomando de interfaz que establece el valor del intervalo Hello para ese proceso EIGRP.
ip hold-time eigrp *número-as valor-temporizador*	Subcomando de interfaz que establece el valor del temporizador de espera EIGRP para esa interfaz.
maximum-paths *número-de-rutas*	Subcomando de router que define el número máximo de rutas de igual coste que se pueden añadir a la tabla de enrutamiento.
ip authentication key-chain eigrp *as nombre-cadena*	Subcomando de interfaz que hace referencia a la cadena de claves utilizada para la autenticación MD5 con EIGRP.
ip authentication mode eigrp *asn* md5	Subcomando de interfaz que activa la autenticación MD5 EIGRP para todos los vecinos a los que se llegue desde la interfaz.
key chain *nombre*	Comando global que sirve para crear y nombrar una cadena de claves de autenticación.
key *número-entero*	Comando de modo de cadena de claves, para crear un nuevo número de clave.
key-string *texto*	Comando de modo de cadena de claves para crear el valor de la clave de autenticación.
accept-lifetime *instante-inicial* {infinite | *instante-final* | duration *segundos*}	Comando del modo de cadena de claves para establecer el intervalo temporal durante el que un router admitirá el uso de una determinada clave.
send-lifetime *instante-inicial* {infinite | *instante-final* | duration *segundos*}	Comando del modo de cadena de claves que sirve para especificar el intervalo de tiempo durante el cual un router enviará mensajes EIGRP empleando una determinada clave.

Tabla 10.6. Comandos EXEC del Capìtulo 10.

Comando	Descripción
show ip route eigrp	Muestra las rutas de la tabla de enrutamiento que se han aprendido mediante EIGRP.
show ip route *dirección-IP* [*máscara*]	Muestra toda la tabla de enrutamiento, o un subconjunto si se introducen parámetros.

(continúa)

Tabla 10.6. Comandos EXEC del Capìtulo 10 *(continuación).*

Comando	Descripción
show ip protocols	Muestra los parámetros del protocolo de enrutamiento y los valores actuales de los temporizadores.
show ip eigrp neighbors	Muestra los vecinos EIGRP y su estado.
show ip eigrp topology	Muestra el contenido de la tabla topológica EIGRP, incluyendo los sucesores y sucesores factibles.
show ip eigrp trafic	Muestra estadísticas relativas al número de mensajes EIGRP enviados y recibidos por un router.
debug eigrp packets	Muestra el contenido de los paquetes EIGRP.
debug eigrp fsm	Muestra los cambios habidos en las rutas sucesora y sucesora factible EIGRP.
debug ip eigrp	Muestra un resultado similar al de debug eigrp packets, pero específicamente para IP.

Este capítulo trata los siguientes temas:

Perspectivas para la resolución de problemas con los protocolos de enrutamiento: Esta breve sección introductoria explica el proceso de resolución de problemas que se sugiere en este libro para problemas relacionados con los protocolos de enrutamiento.

Interfaces habilitadas para un protocolo de enrutamiento: Esta sección muestra la forma de determinar las interfaces a través de las que los routers intentan formar relaciones de vecindad, y cuyas subredes conectadas publican.

Relaciones de vecindad: Esta sección examina por qué los routers no llegan a hacerse vecinos de routers de los que deberían hacerse vecinos.

CAPÍTULO 11

Resolución de problemas en los protocolos de enrutamiento

Los Capítulos 3 y 7, que son los otros dos capítulos del libro dedicados a la resolución de problemas, se centran en el proceso de envío de datos. En particular, el Capítulo 7, "Resolución de problemas de enrutamiento IP", ignora casi por completo la forma en que se añaden rutas a la tabla de enrutamiento, y se centra totalmente en el proceso del plano de datos del envío de paquetes IP, y en la forma de resolver problemas asociados a ese proceso. El Capítulo 7 supone que los procesos del plano de control relacionados con rellenar la tabla de enrutamiento se tratarán en otra parte; esto se hará principalmente en la Parte III del libro.

Este capítulo finaliza el tratamiento del plano de control de IPv4 (el proceso mediante el cual se rellenan las tablas de enrutamiento de los routers con buenas rutas), examinando la forma de resolver problemas relacionados con OSPF e EIGRP. El proceso de resolución de problemas es relativamente sencillo, al menos hasta el nivel requerido para los exámenes de CCNA. Sin embargo, como de costumbre, cuando se resuelven problemas es necesario pensar en muchos detalles distintos, así que el proceso puede servir de ayuda para asegurar que se verifican todos los componentes antes de pasar a la función siguiente.

Este capítulo pone fin a la Parte III del libro. Si se está preparando especialmente para el examen de CCNA siguiendo el plan de lectura mencionado en la Introducción, obsérvese que después de este capítulo debería volver a la Parte IV del libro **CCENT/CCNA ICND1**.

Cuestionario "Ponga a prueba sus conocimientos"

Los capítulos relacionados con la resolución de problemas de este libro se basan en conceptos tomados de muchos otros capítulos, incluyendo algunos del libro **CCENT/CCNA ICND1**. También muestran la forma de enfocar algunas de las cuestiones más difíciles de los exámenes CCNA. Por tanto, es bueno leer estos capítulos independientemente del gra-

do de conocimiento que se tenga. Por estas razones, los capítulos de resolución de problemas no contiene el cuestionario "Ponga a prueba sus conocimientos". Sin embargo, si realmente confía en que podrá abordar la resolución de problemas de OSPF y EIGRP, no lo dude y pase a la sección "Ejercicios para la preparación del examen" que se encuentra cerca del final de este capítulo, descartando así la mayor parte del capítulo.

Temas fundamentales

El mejor primer paso cuando se aborda la resolución de problemas de un protocolo de enrutamiento consiste en examinar la configuración de los distintos routers. Al comparar la configuración del protocolo de enrutamiento, y especialmente los subcomandos `network`, con las direcciones IP de las interfaces, se puede confirmar rápidamente si el protocolo de enrutamiento se ha habilitado en todas las interfaces deseadas. Si el protocolo está habilitado en todas las interfaces correctas de todos los routers, un examen posterior de la configuración de la interfaz y de la configuración de autenticación puede verificar si ciertos ajustes de configuración podrían evitar que dos routers de la misma subred se hiciesen vecinos. Dos routers no podrán intercambiar información de enrutamiento si no satisfacen todos los requisitos necesarios para llegar a ser vecinos.

El Capítulo 9, "OSPF", y el Capítulo 10, "EIGRP", describen extensamente la configuración de los protocolos de enrutamiento, así que este capítulo no intentará explicar la forma de resolver un problema buscando errores de configuración. Sin embargo, la configuración puede no estar siempre disponible en los exámenes, o en la vida real. Este capítulo se centra en resolver problemas con los protocolos de enrutamiento empleando únicamente los comandos `show` y `debug`. En primer lugar, el capítulo describe algunas opciones para resolver problemas de los protocolos de enrutamiento, incluyendo una sugerencia de proceso que tiene dos pasos principales. Las otras dos secciones principales de este capítulo examinan la forma de llevar a cabo cada uno de los pasos principales de la resolución de problemas, tanto para EIGRP como para OSPF.

Perspectivas para la resolución de problemas con los protocolos de enrutamiento

Como la tarea de un protocolo de enrutamiento consiste en rellenar la tabla de enrutamiento del router con las mejores rutas en cada momento, tiene sentido empezar la resolución de problemas potenciales de los protocolos de enrutamiento que pudieran empezar en la tabla de enrutamiento IP. Dada una información básica respecto a la red, incluyendo los routers, sus máscaras y direcciones IP, y el protocolo de enrutamiento, se podrían calcular los números de las subredes que debieran estar en la tabla de enrutamiento del rou-

ter, y se podría determinar el probable router o routers que serían el siguiente salto para cada ruta. Por ejemplo, la Figura 11.1 muestra una internetwork con seis subredes. La tabla de enrutamiento del Router R1 debería mostrar las seis subredes, con tres rutas conectadas, dos rutas aprendidas de R2 (172.16.4.0/24 y 172.16.5.0/24), y con una ruta aprendida de R3 (172.16.6.0/24).

Por tanto, un posible proceso de resolución de problemas consiste en analizar la internetwork, examinar la tabla de enrutamiento y buscar rutas que falten. Si falta una o más rutas, el paso siguiente será determinar si ese router ha aprendido alguna ruta del router del que se espera que sea el siguiente salto (un router vecino). Los pasos siguientes para aislar el problema varían mucho si el router tiene problemas para formar una relación de vecindad con otro router, o si se tiene una relación de vecindad pero no resulta posible aprender todas las rutas.

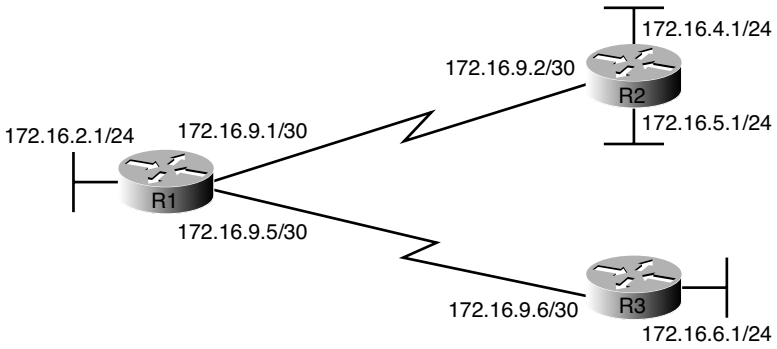


Figura 11.1. Una internetwork con seis subredes

Por ejemplo, imagine que en la Figura 11.1 el router R1 ha aprendido una ruta que va a la subred 172.16.4.0/24 de esta Figura 11.1 pero no para la subred 172.16.5.0/24. En este caso, está claro que R1 tiene una relación de vecindad operativa con R2. En estos casos, la causa raíz del problema puede seguir estando relacionada con el protocolo de enrutamiento, o puede no estar relacionada con dicho protocolo. Por ejemplo, el problema podría ser que la interfaz LAN inferior de R2 está desactivada. Sin embargo, si R1 no tuviera una ruta para llegar a 172.16.4.0/24 o a 172.16.5.0/24, el problema podría ser la relación de vecindad de R1 con R2.

La resolución de problemas de los protocolos de enrutamiento en redes reales puede volverse muy compleja, de hecho puede ser mucho más compleja que las más difíciles de las preguntas del examen de CCNA. La definición de un proceso genérico para la resolución de problemas mediante el cual se puedan abordar tanto problemas de protocolos de enrutamiento simples como complejos requeriría mucho espacio, y sería contraproducente para preparar los exámenes de CCNA. Este capítulo ofrece un proceso sencillo para atacar problemas con los protocolos de enrutamiento; específicamente para problemas cuyo nivel y complejidad son similares a los de los exámenes CCNA.

Si una pregunta del examen parece estar relacionada con un protocolo de enrutamiento, se pueden identificar rápidamente algunos errores comunes de configuración mediante el proceso siguiente, aunque no se disponga de la configuración o no se pueda utilizar el comando show running-config. El proceso posee tres ramas principales:

Paso 1 Examine el diseño de la red para determinar en cuales de las interfaces debería estar habilitado el protocolo de enrutamiento, y cuales son los routers de los que se espera que se hagan vecinos.

Paso 2 Verifique si el protocolo de enrutamiento está habilitado en todas las interfaces (según se dice en el Paso 1). De no ser así, determine la causa inicial y corrija el problema.

Paso 3 Verifique que cada router haya formado todas las relaciones de vecindad especificadas. De no ser así, busque la causa inicial y corrija el problema.

En este momento, habiendo terminado los Capítulos 9 y 10, el Paso 1 no debería requerir más explicaciones. Las dos secciones principales que quedan en este capítulo examinan los Pasos 2 y 3. Completando estos pasos y corrigiendo los posibles problemas hallados mediante este proceso, deberían quedar corregidos los problemas relacionados con el protocolo de enrutamiento propios del nivel CCNA.

Interfaces habilitadas para un protocolo de enrutamiento

Esta sección examina el segundo de los pasos principales para la resolución de problemas que se esbozaban en la sección anterior del capítulo: la forma de verificar las interfaces en las que se ha habilitado el protocolo de enrutamiento. Tanto la configuración de EIGRP como la de OSFP activan el protocolo de enrutamiento en una interfaz empleando el subcomando de router network. Para aquellas interfaces que se vean afectadas por los comandos network, el protocolo de enrutamiento prueba las dos acciones siguientes:

- Intenta hallar vecinos potenciales en la subred que está conectada a la interfaz.
- Publica la subred que está conectada a esta interfaz.

Al mismo tiempo, el subcomando de router passive-interface se puede configurar de tal modo que el router no intente buscar vecinos en la interfaz (que es la primera de las acciones que se acaban de indicar), pero de manera que siga publicando la subred conectada (que es la segunda acción).

Lo único que se necesita para saber exactamente qué interfaces se han habilitado con EIGRP y OSPF, y qué interfaces son pasivas, son tres comandos show. En particular, el comando show ip eigrp interfaces muestra todas las interfaces habilitadas con EIGRP que no son pasivas. El comando show ip protocols muestra, en esencia, el contenido de los comandos network configurados para cada protocolo de enrutamiento, así como una lista por separado que contiene las interfaces pasivas. Al comparar estos dos comandos se identifican todas las interfaces en que está activado EIGRP, y las que son pasivas. Para OSPF, el

comando funciona de forma ligeramente distinta, y concretamente el comando show ip ospf interface brief enumera todas las interfaces en que está habilitado OSPF (incluyendo las interfaces pasivas). La Tabla 11.1 resume estos comandos para disponer de una sencilla referencia.

Tabla 11.1. Comandos clave para hallar las interfaces con un protocolo de enrutamiento habilitado.

Comando	Información clave
show ip eigrp interfaces	Muestra las interfaces en que está habilitado el protocolo de enrutamiento (basándose en comandos network), salvo las interfaces pasivas.
show ip ospf interface brief	Muestra las interfaces en que está habilitado OSPF (basándose en comandos network), incluyendo las interfaces pasivas.
show ip protocols	Muestra el contenido de los comandos de configuración network para cada proceso de enrutamiento, y también las interfaces habilitadas pero pasivas.

Nota

Todos los comandos de la Tabla 11.1 muestran las interfaces independientemente del estado de la interfaz, así que a todos los efectos muestran el resultado de los comandos de configuración network y passive-interface.

Por tanto, para el paso principal de resolución de problemas que se trata en esta sección, la tarea consiste en utilizar los comandos de la Tabla 11.1 y analizar la salida. Primero se mostrará un ejemplo de EIGRP y después un ejemplo de OSPF.

Ejemplo de resolución de problemas en una interfaz EIGRP

Esta sección muestra unos pocos ejemplos de estos comandos en el contexto de la Figura 11.2, que se utiliza en todos los ejemplos de este capítulo.

Este ejemplo contiene cuatro routers, y en este caso el escenario es como sigue:

- R1 y R2 están configurados correctamente en ambas interfaces LAN.
- Por equivocación, R3 no tiene habilitado EIGRP en su interfaz Fa0/1.
- R4 iba a utilizar un comando passive-interface fa0/1, porque no hay otros routers en la Fa0/1 LAN de R4, pero en su lugar R4 se he configurado con el comando passive-interface fa0/0.

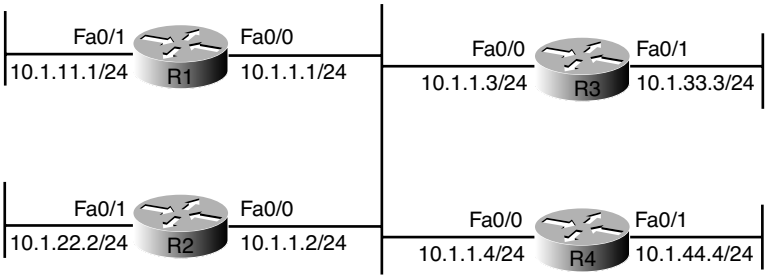


Figura 11.2. Internetwork que se emplea como base para todos los ejemplos de resolución de problemas en EIGRP y OSPF.

El Ejemplo 11.1 empieza mostrando los comandos pertinentes, con un ejemplo en R1 o en R2. También muestra la configuración en R1 para poder hacer una comparación.

Ejemplo 11.1. Problemas de EIGRP con las interfaces.

```
R1#show running-config
! Sólo se muestran las líneas pertinentes
router eigrp 99
network 10.0.0.0
!
R1>show ip eigrp interfaces
IP-EIGRP interfaces for process 99

                    Xmit Queue    Mean   Pacing Time   Multicast    Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0         2       0/0         620       0/10          50           0
Fa0/1         0       0/0           0       0/10           0           0
R1>show ip eigrp protocol
Routing Protocol is "eigrp 99"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 99
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Routing Information Sources:
    Gateway      Distance       Last Update
    10.1.1.2           90       00:13:11
    10.1.1.3           90       00:13:09
```

(continúa)

Ejemplo 11.1. Problemas de EIGRP con las interfaces *(continuación)*.

```
 Distance: internal 90 external 170
! Los próximos comandos se ejecutan en el Router R2
!
R2>show ip eigrp interfaces
IP-EIGRP interfaces for process 99

                      Xmit Queue    Mean   Pacing Time   Multicast    Pending
Interface    Peers    Un/Reliable   SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0          2          0/0        736       0/1          3684         0
Fa0/1          0          0/0          0       0/1             0         0
R2>show ip protocols
Routing Protocol is "eigrp 99"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 99
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Routing Information Sources:
   Gateway         Distance      Last Update
   10.1.1.3              90      00:13:25
   10.1.1.1              90      00:13:25
  Distance: internal 90 external 170

R2>show ip route eigrp
      10.0.0.0/24 is subnetted, 3 subnets
D        10.1.11.0 [90/30720] via 10.1.1.1, 00:13:38, FastEthernet0/0
```

La salida del comando show ip eigrp interfaces en R1 y R2 muestra que R1 y R2 tienen configurado EIGRP empleando el ID de proceso 99, y que EIGRP se ha habilitado tanto en Fa0/0 como en Fa0/1 en los routers R1 y R2. Este comando sólo muestra las interfaces en las que se ha habilitado EIGRP, excluyendo las interfaces pasivas.

Las partes resaltadas de la salida del comando show ip protocols en cada router son especialmente interesantes. Estas secciones muestran los parámetros de los comandos network usados en la configuración. Para cada comando network, el comando show ip protocols muestra una línea distinta bajo el encabezado "Routing for Networks", y cada línea muestra el contenido de los diferentes subcomandos de router network. Por ejemplo, R1 utiliza el comando de configuración network 10.0.0.0 (que aparece al principio del ejemplo), que coincide con la línea "10.0.0.0" de la salida del comando show ip protocols.

El final del ejemplo da una pequeña idea del problema que hay en R3 desde la perspectiva de R2. El final del comando show ip protocols que hay en R2 muestra dos fuentes de información de enrutamiento: 10.1.1.1 (R1) y 10.1.1.3 (R3). Sin embargo, R2 sólo ha aprendido una ruta EIGRP (10.1.11.0/24), según muestra la salida del comando show ip route eigrp. Cuando funcione correctamente, R2 deberá aprender tres rutas EIGRP, una para cada una de las subredes LAN exteriores que se muestran en la Figura 11.2.

A continuación, el Ejemplo 11.2 muestra los problemas que hay en R3 y R4 que impiden a R1 y R2 aprender la existencia de las subredes 10.1.33.0/24 y 10.1.44.0/24. El ejemplo muestra la configuración pertinente de cada router para disponer de una perspectiva, y también los comandos show que ponen de manifiesto los problemas.

Ejemplo 11.2. Problemas de EIGRP en R3 y R4.

```
R3#show running-config
! Se han omitido ciertas líneas por brevedad
router eigrp 99
  network 10.1.1.3 0.0.0.0
  network 10.1.13.3 0.0.0.0
  auto-summary
R3#show ip eigrp interfaces
IP-EIGRP interfaces for process 99

                      Xmit Queue    Mean   Pacing Time   Multicast    Pending
Interface   Peers     Un/Reliable   SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0         2         0/0           1       0/10          50          0
R3#show ip protocols
Routing Protocol is "eigrp 99"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 99
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.1.1.3/32
    10.1.13.3/32
  Routing Information Sources:
    Gateway      Distance     Last Update
    10.1.1.2           90     00:28:16
    10.1.1.1           90     00:28:14
```

(continúa)

Ejemplo 11.2. Problemas de EIGRP en R3 y R4 *(continuación).*

```
  Distance: internal 90 external 170
! La salida de R4 comienza aquí

R4#show running-config
! Se han omitido líneas por brevedad
router eigrp 99
  passive-interface FastEthernet0/0
  network 10.0.0.0
  auto-summary

R4#show ip eigrp interfaces
IP-EIGRP interfaces for process 99

                     Xmit Queue    Mean   Pacing Time   Multicast    Pending
Interface   Peers    Un/Reliable   SRTT   Un/Reliable   Flow Timer   Routes
Fa0/1         0          0/0          0       0/1           0           0
R4#show ip protocols
Routing Protocol is "eigrp 99"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 99
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Passive Interface(s):
    FastEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

La causa principal del problema de R3 es que R3 tiene un comando de configuración network 10.1.13.3 0.0.0.0, que no coincide con la dirección IP Fa0/1 10.1.33.3 de R3. Si la configuración no estuviera disponible en la pregunta de examen, habría que utilizar el comando show ip protocols para apreciar, en esencia, los mismos detalles de configuración. En este caso, el comando show ip protocols en R3 muestra el texto "10.1.13.3/32" como referencia del contenido de los parámetros del comando network incorrecto. Como resultado, R3 no intenta hallar vecinos en su interfaz Fa0/1, lo cual no tiene mucha importancia en este caso, pero además R3 no publica la subred 10.1.33.0/24, que es la subred que está conectada a su interfaz Fa0/1. Obsérvese también que el comando show ip eigrp interfaces

de R3 omite la interfaz Fa0/1, lo cual en sí mismo no determina la causa principal, pero puede servir de ayuda para aislar el problema.

En R4, el ingeniero podría haber empleado correctamente el subcomando de router passive-interface fastethernet0/1, porque no debería existir ningún router conectado a la interfaz Fa0/1 de R4. Sin embargo, el ingeniero aludió por error a la interfaz Fa0/0 de R4, en lugar de referirse a Fa0/1. El comando show ip eigrp interfaces de R4 omite deliberadamente la interfaz pasiva (Fa0/0), y la parte resaltada del comando show ip protocols de R4 muestra a Fa0/0 como interfaz pasiva. Como Fa0/0 de R4 es pasiva, R4 ni siquiera intenta establecer una relación de vecindad con otros routers de esa misma LAN.

Ejemplo de resolución de problemas en una interfaz

OSPF tiene los mismos requisitos básicos que EIGRP para las interfaces, con algunas salvedades. En primer lugar, los routers EIGRP necesitan utilizar el mismo ASN o ID de proceso que sus routers vecinos, según se haya establecido en el comando global de configuración router. Los routers OSPF pueden utilizar cualquier ID de proceso, sin necesidad de que coincida con el de sus vecinos. En segundo lugar, OSPF requiere que las interfaces conectadas a la misma subred tengan asignada la misma área de OSPF, mientras que en EIGRP no existe el concepto de área.

El Ejemplo 11.3 muestra una internetwork OSPF que casi funciona, basada una vez más en la Figura 11.2. Existen los problemas siguientes:

R2 ha sido configurado para poner ambas interfaces en el área 1. R1, R3 y R4 se han configurado para que pongan sus interfaces LAN comunes (Fa0/0 en todos los casos) en el área 0, lo cual va contra las reglas de diseño de OSPF.

El Ejemplo 11.3 muestra la forma de aislar la causa raíz del problema. También muestra la salida operativa normal obtenida mediante los comandos show ip ospf interface brief y show ip protocols.

Ejemplo 11.3. Problemas de OSPF en R2.

```
R1>show ip ospf interface brief
Interface    PID     Area            IP Address/Mask    Cost    State     Nbrs F/C
Fa0/1        11      0               10.1.11.1/24       1       DR        0/0
Fa0/0        11      0               10.1.1.1/24        1       DROTH     2/2
R1>show ip protocols
Routing Protocol is "ospf 11"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
 Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
```

(continúa)

Ejemplo 11.3. Problemas de OSPF en R2 *(continuación)*.

```
  Routing for Networks:
    10.0.0.0 0.255.255.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:01:12
    4.4.4.4              110      00:01:12
    1.1.1.1              110      00:01:12
  Distance: (default is 110)
R1>show ip route ospf
     10.0.0.0/24 is subnetted, 5 subnets
O       10.1.44.0 [110/2] via 10.1.1.4, 00:01:19, FastEthernet0/0
O       10.1.33.0 [110/2] via 10.1.1.3, 00:01:19, FastEthernet0/0
```

```
! Ahora pasamos al router R2
R2>show ip ospf interface brief
Interface    PID     Area            IP Address/Mask    Cost    State   Nbrs F/C
Fa0/1        22      1               10.1.22.2/24       1       DR      0/0
Fa0/0        22      1               10.1.1.2/24        1       DR      0/0
R2>show ip protocols
Routing Protocol is "ospf 22"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
 --More-- _________ _________ Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.0.0 0.255.255.255 area 1
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
Distance: (default is 110)
R2>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
May 28 18:30:26.659: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID,
from backbone area must be virtual-link but not found from 10.1.1.4,
FastEthernet0/0
```

Para OSPF, el comando show ip ospf inerface brief muestra una salida parecida a la del comando show ip eigrp interface, con una línea por cada interfaz habilitada. (El comando show ip ospf interface, que no se muestra en el ejemplo, muestra información OSPF detallada de todas las interfaces.) En este ejemplo, tanto R1 como R2 tienen habilitado OSPF en ambas interfaces LAN, pero este comando también muestra el número de área para todas las interfaces, y R2 tiene ambas interfaces LAN en el área 1. Como resultado, la interfaz Fa0/0 de R2 está en una área distinta de la que ocupan las otras tres interfaces del router en esa misma LAN.

Un examen más detallado de la salida del comando show ip protocols de R2, y en particular de la parte resaltada, señala el error de configuración. La frase resaltada "10.0.0.0

0.255.255.255 area 1" es en realidad la sintaxis exacta de un comando network del router R2, a falta de la palabra "network". Si se reconfigurase R2 para que su interfaz Fa0/0 coincidiera con los otros tres routers se resolvería este problema en particular.

El final del ejemplo muestra un mensaje de registro no solicitado que genera el Router R2, notificando al usuario de la consola que este router ha recibido un Hello de un router situado en una área distinta.

Cuando compruebe la configuración de las interfaces, debería comprobar también otros detalles que se mencionan en la sección de resolución de problemas de IP del Capítulo 7. Tiene sentido comprobar directamente las direcciones IP de la interfaz, así como sus máscaras y el estado de la interfaz, empleando los comandos show interfaces y show ip interface brief. En particular, sirve de ayuda tomar nota de las interfaces que están en estado *up/up*, porque los protocolos de enrutamiento no intentarán buscar vecinos ni publicarán las subredes de aquellas interfaces que no se encuentren en el estado *up/up*. Estas comprobaciones de verificación se tratan con detalle en el Capítulo 7, así que no se repetirán aquí.

Relaciones de vecindad

Según se mencionaba al principio de este capítulo, cuando se ha habilitado un protocolo de enrutamiento en una interfaz, y la interfaz no está configurada como interfaz pasiva, el protocolo de enrutamiento intenta descubrir vecinos y formar relaciones de vecindad con todos los vecinos que compartan una subred común. Esta sección examina el elevado número de hechos que tiene que comprobar cada router en los vecinos potenciales antes de que dos routers puedan hacerse vecinos.

OSPF e EIGRP utilizan mensajes Hello para conocer la existencia de nuevos vecinos y para intercambiar información que sirve para efectuar algunas comprobaciones básicas. Por ejemplo, tal como se muestra en el Ejemplo 11.3, los routers OSPF no deberían hacerse vecinos de routers de otra área, porque todos los routers de una subred común deben pertenecer a la misma área por diseño. (La frontera entre áreas es un router, no un enlace.)

Una vez que un router EIGRP o OSPF escucha un Hello de un nuevo vecino, el protocolo de enrutamiento examina la información presente en el Hello, junto con ciertos ajustes locales, para decidir si los dos routers deben ni siquiera intentar ser vecinos. Como no existe un término formal que denote todos estos ajustes que consideran los protocolos de enrutamiento, este libro los denomina **requisitos de vecindad**. La Tabla 11.2 muestra los requisitos de vecindad para EIGRP y para OSPF. Después de la tabla, las páginas siguientes examinan algunos de estos ajustes para EIGRP y OSPF, empleando de nuevo ejemplos basados en la Figura 11.2.

Nota

Aunque es importante estudiar y recordar las indicaciones de esta tabla, quizá no sea lo mejor estudiar la tabla en este preciso momento. Es conveniente leer antes el resto del capítulo, porque los elementos de la tabla se mencionarán y revisarán a lo largo del resto del capítulo.

Tabla 11.2. Requisitos de vecindad para EIGRP y OSPF.

Requisito	EIGRP	OSPF
Las interfaces tienen que hallarse en el estado *up*/*up*	Sí	Sí
Las interfaces deben hallarse en la misma subred	Sí	Sí
Hay que pasar la autenticación de vecinos (si está configurada)	Sí	Sí
Tienen que usar el mismo ASN/ID de proceso que se haya especificado en el comando de configuración router	Sí	No
Tienen que coincidir los temporizadores Hello y espera/muerto	No	Sí
La MTU IP tiene que coincidir	No	Sí
Los IDs de router tienen que ser exclusivos	No[1]	Sí
Los valores-K deben coincidir	Sí	N/A
Tienen que estar en la misma área	N/A	Sí

[1] Tener RIDs de EIGRP duplicadas no impide que los routers se hagan vecinos, pero puede dar lugar a problemas cuando se añadan rutas EIGRP externas a la tabla de enrutamiento.

A diferencia de los demás requisitos de vecindad que se muestran en la Tabla 11.2, el primer requisito tiene muy poco que ver con los protocolos de enrutamiento en sí. Los dos routers deben ser capaces de enviarse paquetes entre sí a través de la red física a la que están conectados. Para hacer esto, las interfaces de los routers tienen que estar *up*/*up*. En la práctica, antes de examinar otros detalles por los cuales dos routers puedan no hacerse vecinos, asegúrese de que ambos routers se puedan enviar un ping entre sí en la subred local. Si falla el ping, investigue todos los problemas de las capas 1, 2 y 3 que pudieran evitar que funcione el ping (tales como una interfaz que no esté *up*/*up*), según se ha descrito en varios capítulos de este libro y del libro **CCENT/CCNA ICND1**.

Como los detalles difieren ligeramente entre los dos protocolos de enrutamiento, esta sección examina primero EIGRP y después OSPF.

Nota

Esta sección supone que el protocolo de enrutamiento ya se ha habilitado en todas las interfaces necesarias, según se describe en la sección "Interfaces habilitadas para un protocolo de enrutamiento".

Requisitos de vecindad en EIGRP

Cualquier pareja de routers EIGRP que se conecten a un mismo enlace de datos y cuyas interfaces se hayan habilitado para EIGRP y no sean pasivas considerarán, como mínimo,

la posibilidad de hacerse vecinos. Para saber de forma rápida y definitiva qué vecinos potenciales han pasado todos los requisitos de vecindad para EIGRP, basta examinar la salida del comando show ip eigrp neighbors. Este comando sólo muestra aquellos vecinos que han pasado todas las comprobaciones de verificación de vecindad. El Ejemplo 11.4 muestra un ejemplo, con los cuatro routers de la Figura 11.2, pero después de haber corregido todos los problemas anteriores de configuración de EIGRP.

Ejemplo 11.4. El comando **show ip eigrp neighbors** de R1 con todos los problemas corregidos.

```
SR1#show ip eigrp neighbors
IP-EIGRP neighbors for process 99
H     Address      Interface     Hold Uptime    SRTT     RTO      Q      Seq
                                 (sec)          (ms)             Cnt    Num
2     10.1.1.3     Fa0/0         13 00:00:04    616     3696      0      8
1     10.1.1.4     Fa0/0         12 00:00:54      1      200      0      45
0     10.1.1.2     Fa0/0         14 00:01:19    123      738      0      43
```

Si el comando show ip eigrp neighbors no muestra uno o más vecinos esperados, y los dos routers pueden hacer un ping a la dirección IP del otro en su subred común, es probable que el problema esté relacionado con uno de los requisitos de vecindad que se enumeran en las Tablas 11.2 y 11.3. La Tabla 11.3 resume los requisitos de vecindad de EIGRP y muestra los comandos más apropiados para determinar cual de los requisitos es la causa inicial del problema.

Tabla 11.3. Requisitos de vecindad de EIGRP y comandos **show/debug** más apropiados.

Requisito	Mejor(es) comando(s) para aislar el problema
Deben estar en la misma subred	show interfaces
Deben pasar la autenticación de vecinos	debug eigrp packets
Deben usar el mismo ASN en el comando de configuración router	show ip eigrp interfaces, show protocols
Los valores K deben coincidir	show protocols

Todos los requisitos que se enumeran en la Tabla 11.3, salvo el último, se han explicado en el Capítulo 10. Los valores K de EIGRP se refieren a los parámetros que se pueden configurar para modificar lo que utiliza EIGRP en sus cálculos de métricas. Cisco recomienda dejar estos ajustes con sus valores iniciales, empleando únicamente el ancho de banda y el retardo para calcular las métricas. Como Cisco recomienda no modificar esos valores, este problema en particular no es muy frecuente. Sin embargo, se pueden comprobar los valores K de ambos routers empleando el comando show ip protocols.

El Ejemplo 11.5 muestra tres problemas que pueden dar lugar a que dos routers que debieran hacerse vecinos EIGRP no lleguen a hacerlo. Para este ejemplo se han introducido los problemas siguientes:

- Se ha configurado R2 con la dirección IP 10.1.2.2/24, que está en una subred distinta a la de R1, R3 y R4.
- Se ha configurado R3 para que utilice el ASN 199 mediante el comando router eigrp 199, en lugar de usar el ASN 99, que es lo que se hace en los otros tres routers.
- Se ha configurado R4 para utilizar la autenticación MD5, como los otros routers, pero R4 tiene el valor clave "FRED" en lugar del valor "fred", que es el que utilizan los otros tres routers.

R1 puede detectar dos de los problemas sin tener que utilizar comandos en los otros routers. R1 genera un mensaje de registro no solicitado para el problema de la red que no coincide, y un comando debug en R1 puede revelar el fallo de autenticación. Un rápido examen de unos cuantos comandos show en R3 puede identificar que se ha empleado un ASN incorrecto en el comando de configuración router. El Ejemplo 11.5 muestra los detalles.

Ejemplo 11.5. Problemas comunes que impiden la formación de vecinos EIGRP.

```
! Al principio, R1 no tiene relaciones de vecindad. R1 emplea el ASN (proceso) 99.
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 99

R1#
! A continuación, R1 genera un mensaje de registro que aparece en la consola,
! e indica que el router cuya dirección IP es 10.1.2.2 no está en la misma
! subred que R1.
!
*May 28 20:02:22.355: IP-EIGRP(Default-IP-Routing-Table:99): Neighbor
    10.1.2.2 not on common subnet for FastEthernet0/0

! Después, R1 habilita un debug que muestra mensajes para todos los paquetes
! recibidos de R4, que emplea una contraseña incorrecta (cadena
! clave de autenticación)
!
R1#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
     SIAREPLY)
*May 28 20:04:00.931: EIGRP: pkt key id = 1, authentication mismatch
*May 28 20:04:00.931: EIGRP: FastEthernet0/0: ignored packet from 10.1.1.4,
  opcode = 5 (invalid authentication)
! El resto de la salida es desde R3
! La primera línea de la salida de show ip protocols muestra el ASN 199
!
R3#show ip protocols
Routing Protocol is "eigrp 199"
!
! La primera línea de la salida de show ip eigrp interfaces muestra el ASN 199
!
R3#show ip eigrp interfaces
IP-EIGRP interfaces for process 199

                    Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface   Peers   Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0         0         0/0        0       0/10          0          0
Fa0/1         0         0/0        0       0/10          0          0
```

Requisitos de vecindad en OSPF

De forma similar a EIGRP, el comando show ip ospf neighbor ejecutado en un router muestra todos los routers vecinos que han cumplido los requisitos necesarios para pasar a ser vecinos OSPF, según se indican en la Tabla 11.2; hay una pequeña excepción, que es una MTU que no coincide. (Si no coincide la MTU, los dos routers se muestran en el comando show ip ospf neighbor. Este problema concreto se discute más adelante, en la sección "El requisito de igualdad de MTU.") Por tanto, el primer paso para la resolución de problemas relativos a la vecindad en OSPF es examinar la lista de vecinos.

El Ejemplo 11.6 muestra la salida del comando show ip ospf neighbor en el router R2, de la Figura 11.2, con una configuración correcta en los cuatro routers de la figura.

Ejemplo 11.6. Resultado del comando **show ip ospf neighbors** en el router R2 en condiciones normales de funcionamiento.

```
R2#show ip ospf neighbor

Neighbor ID     Pri     State           Dead Time     Address       Interface
1.1.1.1           1     FULL/BDR        00:00:37      10.1.1.1      FastEthernet0/0
3.3.3.3           1     2WAY/DROTHER    00:00:37      10.1.1.3      FastEthernet0/0
4.4.4.4           1     FULL/DR         00:00:31      10.1.1.4      FastEthernet0/0
```

Una breve revisión de los estados de vecindad OSPF (según se explicaba en el Capítulo 9) puede servir de ayuda para comprender algunas sutilezas del ejemplo. El estado que muestra un router de cada uno de sus vecinos OSPF (el estado del vecino) debería llegar a ser o bien *two-way* (bidireccional) o bien *Full* en condiciones normales de funcionamiento. Para los vecinos que no necesitan intercambiar directamente sus bases de datos, y que normalmente son los routers de una LAN que no son DR, los routers deberían llegar a estar en un estado de vecindad *two-way*. En la mayoría de los casos, los dos routers vecinos necesitan intercambiar directamente sus LSDBs completas entre sí. Una vez completado ese proceso, los dos routers pasan al estado de vecindad *Full* (completo). En el Ejemplo 11.6, el router R4 es el DR, y R1 es el BDR, así que R2 y R3 (al no ser DR) no necesitan intercambiar rutas directamente. Por tanto, el estado de vecindad de R2 para R3 (RID 3.3.3.3) en el Ejemplo 11.6 se muestra como *two-way*.

Nota

Téngase en cuenta que los vecinos OSPF no necesitan emplear el mismo ID de proceso en el comando router ospf *id-proceso* para hacerse vecinos. En el Ejemplo 11.6, los cuatro routers emplean distintos IDs de proceso.

Si el comando show ip ospf neighbor no muestra a uno o más de los vecinos esperados, antes de pasar a examinar los requisitos de vecindad OSPF se debe confirmar que los dos

routers pueden enviarse respectivamente un ping a través de la subred local. En cuanto puedan hacerlo, si los dos routers siguen sin hacerse vecinos OSPF, el paso siguiente consiste en examinar cada uno de los requisitos de vecindad OSPF. La Tabla 11.4 resume los requisitos, y muestra los comandos más útiles para buscar las respuestas.

Tabla 11.4. Requisitos de vecindad OSPF y comandos **show/debug** más oportunos.

Requisitos	Comandos óptimos para aislar el problema
Debe estar en la misma subred	show interfaces, debug ip ospf hello
Debe pasar la posible autenticación de vecino	debug ip ospf adj
Deben coincidir los temporizadores Hello y espera/muerto	show ip ospf interface, debug ip ospf hello
Debe estar en la misma área	debug ip ospf adj, show ip ospf interface brief
Los IDs de router tienen que ser únicos	show ip ospf

El resto de esta sección examina un par de ejemplos en los cuales dos routers OSPF podrían hacerse vecinos, pero no lo hacen por algunas de las razones que se muestran en la tabla. A continuación se ofrece información sobre el requisito de igualdad de MTU.

Ejemplo 1 de vecindad en OSPF

En este primer ejemplo de problemas de vecindad en OSPF, se utiliza la red habitual con cuatro routers de la Figura 11.2. Esta red se ha diseñado de tal modo que haga uso de una sola área, el área 0. En este caso, se han introducido en el diseño los problemas siguientes:

- R2 se ha configurado con ambas interfaces LAN en el área 1, mientras que las interfaces Fa0/0 de los otros tres routers se han asignado al área 0.
- R3 utiliza el mismo RID (1.1.1.1) que R1.
- R4 utiliza una autenticación MD5 al igual que los otros tres routers, pero R4 tiene mal configurada su clave de autenticación (FRED en lugar de fred).

El Ejemplo 11.7 muestra la evidencia de estos problemas, junto con comentarios a continuación del ejemplo.

Según se indicaba en la Tabla 11.4, el comando debug ip ospf adj sirve de ayuda para resolver problemas relacionados con las áreas de OSPF que no coinciden, y también para abordar problemas de autenticación. Los mensajes resaltados en las primeras líneas del ejemplo ponen de manifiesto que el router cuya dirección es 10.1.1.2 (R2) tiene un ID de área que no coincide, 0.0.0.1, que denota el área 1. Ciertamente, R2 se configuró incorrectamente para poner su interfaz Fa0/0 en el área 1. Inmediatamente después hay una referencia a una "mismatched authentication key" (clave de autenticación nocoincidente), lo

Ejemplo 11.7. Búsqueda de problemas por no coincidencia de áreas, igual RID y problemas de autenticación.

```
R1#debug ip ospf adj
OSPF adjacency events debugging is on
R1#
*May 28 23:59:21.031: OSPF: Send with youngest Key 1
*May 28 23:59:24.463: OSPF: Rcv pkt from 10.1.1.2, FastEthernet0/0, area 0.0.0.0
       mismatch area 0.0.0.1 in the header
*May 28 23:59:24.907: OSPF: Rcv pkt from 10.1.1.4, FastEthernet0/0 :
  Mismatch Authentication Key - Message Digest Key 1

R1#undebug all
All possible debugging has been turned off
R1#show ip ospf interface brief
Interface    PID   Area      IP Address/Mask    Cost    State    Nbrs F/C
Fa0/1        11    0         10.1.11.1/24       1       DR       0/0
Fa0/0        11    0         10.1.1.1/24        1       DR       0/0
! Ahora vamos a R2
! R2 muestra que Fa0/0 está en el área 1
!
R2#show ip ospf interface brief
Interface    PID   Area      IP Address/Mask    Cost    State    Nbrs F/C
Fa0/1        22    1         10.1.22.2/24       1       DR       0/0
Fa0/0        22    1         10.1.1.2/24        1       DR       0/0
! Ahora vamos a R3
! R3 muestra un RID igual a 1.1.1.1
!
R3#show ip ospf
 Routing Process "ospf 33" with ID 1.1.1.1
 Supports only single TOS(TOS0) routes
! Se han omitido líneas por brevedad
! Ahora volvemos a R1
! El comando siguiente confirma que R1 también está
! intentando utilizar el RID 1.1.1.1
!
R1#show ip ospf
 Routing Process "ospf 11" with ID 1.1.1.1
 Supports only single TOS(TOS0) routes
 ! Se han omitido líneas por brevedad
*May 29 00:01:25.679: %OSPF-4-DUP_RTRID_NBR: OSPF detected duplicate router-id
1.1.1.1 from 10.1.1.3 on interface FastEthernet0/0
```

cual significa que se ha empleado el tipo de autenticación correcto, pero las claves tienen distintos valores, específicamente para el router 10.1.1.4 (R4).

Nota

Los routers tratan los mensajes de depuración como mensajes de registro, que son enviados por el IOS a la consola de forma predeterminada. Para visualizar estos mensajes

desde una conexión Telnet o ssh, utilice el comando terminal monitor. Para desactivar la visualización de estos mensajes, utilice el comando terminal no monitor.

La parte siguiente del ejemplo muestra el comando show ip ospf interface brief tanto en R1 como en R2, poniéndose de manifiesto que la interfaz Fa0/0 de cada router se encuentra en un área diferente de OSPF.

El final del ejemplo muestra la información que indica que R1 y R3 intentan utilizar el RID 1.1.1.1. Curiosamente, ambos routers generan automáticamente un mensaje de registro correspondiente al problema de duplicación de RID en OSPF entre R1 y R3. Un RID duplicado da lugar a problemas significativos con OSPF, problemas mucho más graves que la simple cuestión de hacerse o no vecinos. El final del Ejemplo 11.7 muestra resaltado el mensaje de registro. Los comandos show ip ospf, ejecutados en R3 y R1, también muestran que es fácil visualizar el RID de cada router, observándose entonces que ambos utilizan el mismo valor.

Ejemplo 2 de vecindad en OSPF

En este ejemplo se vuelve a utilizar la misma red de la Figura 11.2. Los problemas de R2, R3 y R4 que había en el ejemplo anterior se han corregido, pero se han introducido nuevos problemas en R2 y R4 para mostrar los síntomas correspondientes. En este caso, se han introducido en el diseño los problemas siguientes:

- R2 se ha configurado con un temporizador Hello/Dead de 5/20 en su interfaz Fa0/0, en lugar del 10/40 que se utiliza (de forma predeterminada) en R1, R3 y R4.
- Se han resuelto los problemas de R3; no existen problemas con vecinos OSPF.
- Ahora R4 está empleando la cadena de clave correcta (fred) pero con autenticación de texto plano en lugar de la autenticación MD5 que emplean los otros tres routers.

El Ejemplo 11.8 muestra la evidencia de los problemas; se muestran comentarios después del ejemplo. Como de costumbre, el comando debug ip ospf adj ayuda a descubrir problemas de autenticación. Además, el comando debug ip ospf hello ayuda a descubrir las disparidades observadas en el mensaje Hello, incluyendo las disparidades en direcciones/máscaras IP y en los temporizadores.

El ejemplo comienza con los mensajes de depuración relacionados con el problema de autenticación existente entre R1, que utiliza autenticación MD5, y R4, que ahora utiliza autenticación en texto plano o sin formato. Según se indicaba en la Tabla 9.4 del Capítulo 9, el IOS considera que la autenticación de texto plano en OSPF es de tipo 1 y la autenticación MD5 es de tipo 2. El mensaje de depuración resaltado confirma esta idea, e indica que R1 ha recibido un paquete procedente de 10.1.1.4 (R4), con autenticación de tipo 1, pero R1 esperaba una autenticación de tipo 2.

A continuación, el ejemplo muestra los mensajes generados por el comando debug ip ospf hello (específicamente, los que están relacionados con la disparidad de temporizadores Hello/Dead). El mensaje resaltado utiliza la "C" para denotar "valor configurado"; en otras palabras, el valor del router local, que en este caso es R1. La "R" del mensaje denota "valor recibido", que es el valor que aparce en el mensaje Hello recibido. En este caso, la

Ejemplo 11.8. Búsqueda de temporizadores Hello/Dead que no cinciden, y de tipos de autenticación incorrectos.

```
R1#debug ip ospf adj
OSPF adjacency events debugging is on
R1#
*May 29 10:41:30.639: OSPF: Rcv pkt from 10.1.1.4, FastEthernet0/0 :
Mismatch Authentication type. Input packet specified type 1, we use type 2
R1#
R1#undebug all
All possible debugging has been turned off
R1#debug ip ospf hello
OSPF hello events debugging is on
R1#
*May 29 10:41:42.603: OSPF: Rcv hello from 2.2.2.2 area 0 from
  FastEthernet0/0 10.1.1.2
*May 29 10:41:42.603: OSPF: Mismatched hello parameters from 10.1.1.2
*May 29 10:41:42.603: OSPF: Dead R 20 C 40, Hello R 5 C 10
  Mask R 255.255.255.0 C 255.255.255.0
R1#undebug all
All possible debugging has been turned off
R1#show ip ospf interface fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 10.1.1.1/24, Area 0
  Process ID 11, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 10.1.1.1
  Backup Designated router (ID) 3.3.3.3, Interface address 10.1.1.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
! Se han omitido ciertas líneas por brevedad
```

```
! A continuación pasamos a R2
!
R2#show ip ospf interface fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 10.1.1.2/24, Area 0
  Process ID 22, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 10.1.1.2
  No backup designated router on this network
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
! Se han omitido ciertas líneas
```

frase "Dead R 20 C 40" significa que el router que ha generado este mensaje, el R1, recibió un Hello cuyo temporizador Dead valía 20, pero el valor configurado para R1 en la interfaz es 40, así que no coinciden los valores. De forma similar, el mensaje muestra también la disparidad de los temporizadores Hello. Obsérvese que cualquier problema de disparidad de subredes IP también podría hallare con este mismo comando de depuración, basándose en las máscaras de subred recibidas y configuradas.

La mayor parte del ejemplo muestra la salida del comando show ip ospf interface en R1 y R2, que indica los temporizadores Hello y Dead en las dos interfaces, confirmando los detalles ofrecidos en los mensajes de depuración.

El requisito de igualdad de MTU

De todos los problemas potenciales que hay entre dos vecinos OSPF potenciales, según se muestra en la Tabla 11.2, sólo uno, el de las MTU no coincidentes, permite que el vecino aparezca en la salida del comando show ip ospf neighbor del otro router. Cuando dos routers se conectan a la misma subred, con distintos ajustes de MTU IP en su interfaz, los dos routers pueden hacerse vecinos y alcanzar el estado bidireccional. Sin embargo, cuando los dos routers intentan intercambiar sus LSDB, el proceso de intercambio de bases de datos falla por la discoincidencia de MTU.

Cuando se produce una disparidad de MTU, los routers suelen pasar por unos cuantos estados de vecindad mientras intentan resolver el problema. El estado más común es el estado *Exchange* (intercambio), según se muestra en el Ejemplo 11.9. En este caso, R1 y R3 no tienen otro problema que impida que se hagan vecinos OSPF, salvo que R3 se ha configurado con una MTU IP de 1200 bytes en la interfaz Fa0/0, en lugar de los 1500 (valor predeterminado) que utiliza R1.

Ejemplo 11.9. Resultados de la disparidad de MTU en vecinos OSPF.

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   EXCHANGE/DR     00:00:36    10.1.1.3        FastEthernet0/0
```

Normalmente, el estado efectúa un ciclo que va desde el estado *Exchange* al *Init*, y después al estado *Exchange*.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 11.5 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 11.5. Temas clave para el Capítulo 11

Tema clave	Descripción	Número de página
Lista	Las dos cosas que suceden cuando se habilita EIGRP u OSPF en la interfaz de un router.	412
Tabla 11.1	Lista de tres comandos que son útiles para determinar en qué interfaces se ha activado EIGRP u OSPF.	413
Tabla 11.2	Lista de requisitos de vecindad para EIGRP y para OSPF.	421
Tabla 11.3	Lista de requisitos de vecindad para EIGRP y comandos útiles para aislar el requisito que es la causa inicial de un problema de vecindad.	422
Tabla 11.4	La misma información que en la Tabla 11.3, pero para OSPF.	425

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD), o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas ya completas para validar su trabajo.

Referencias de comandos

Aunque no necesariamente debe memorizar la información de las tablas de esta sección, ésta incluye una referencia de los comandos de configuración y EXEC utilizados en

este capítulo. En la práctica, debería memorizar los comandos como un efecto colateral de leer el capítulo y hacer todas las actividades de esta sección de preparación del examen. Para verificar si ha memorizado los comandos como un efecto secundario de sus otros estudios, cubra el lado izquierdo de la tabla con un trozo de papel, lea las descripciones del lado derecho y compruebe si recuerda el comando.

Tabla 11.6. Comandos de configuración del Capítulo 11.

Comando	Descripción
ip hello-interval eigrp *número-as valor-temporizador*	Subcomando de interfaz que establece el intervalo Hello en EIGRP para ese proceso EIGRP.
ip hold-time eigrp *número-as valor-temporizador*	Subcomando de interfaz que establece el intervalo de espera de EIGRP para esa interfaz.
ip ospf hello-interval *segundos*	Subcomando de interfaz que establece el intervalo para enviar periódicamente mensajes Hello.
ip ospf dead-interval *número*	Subcomando de interfaz que establece el temporizador Dead en OSPF.

Tabla 11.7. Comandos EXEC del Capítulo 11.

Comando	Descripción
show ip protocols	Muestra los parámetros del protocolo de enrutamiento y los valores actuales de los temporizadores, incluyendo una útil copia de los comandos network del protocolo de enrutamiento, y una lista de las interfaces pasivas.
show ip eigrp interfaces	Muestra las interfaces en las que se ha activado EIGRP para cada proceso EIGRP, salvo las interfaces pasivas.
show ip route eigrp	Muestra las rutas de la tabla de enrutamiento aprendidas a través de EIGRP.
debug eigrp packets	Visualiza el contenido de los paquetes EIGRP, incluyendo muchos avisos útiles relativos a las razones por las cuales no llegan a formarse relaciones de vecindad.
show ip eigrp neighbors	Muestra los vecinos EIGRP y su estado.
show ip ospf interface brief	Muestra las interfaces en las que está activado el protocolo OSPF (basándose en comandos network), incluyendo las interfaces pasivas.

(continúa)

Tabla 11.7. Comandos EXEC del Capítulo 11 *(continuación)*.

Comando	Descripción
show ip ospf interface [*tipo número*]	Muestra detalladamente la configuración de OSPF para todas las interfaces, o para la interfaz indicada, incluyendo los temporizadores Hello y Dead, y el área OSPF.
show ip route ospf	Muestra las rutas de la tabla de enrutamiento aprendidas por OSPF.
show ip ospf neighbor	Muestra los vecinos y el estado actual respecto a los vecinos, para cada interfaz.
debug ip ospf events	Emite mensajes de registro para cada acción ejecutada por OSPF, incluyendo la recepción de mensajes.
debug ip ospf packet	Muestra mensajes de error que describen el contenido de todos los paquetes OSPF.
debug ip ospf hello	Emite mensajes de registro que describen los Hellos y los fallos de Hello.

Temas del examen* ICND2 publicados por Cisco que se tratan en esta parte

Configuración y resolución de problemas relativos al funcionamiento básico y el enrutamiento de dispositivos Cisco

- Verificar el funcionamiento del hardware y del software empleando comandos SHOW y DEBUG.

Implementación y verificación de enlaces WAN

- Configuración y verificación de Frame Relay en routers Cisco.
- Resolución de problemas en la implementación de WAN.
- Descripción de la tecnología VPN (importancia, beneficios, rol, impacto, componentes).
- Configuración y verificación de conexiones PPP entre routers Cisco.

* No olvide consultar en http://www.cisco.com los últimos temas de examen publicados.

PARTE IV

Redes de área amplia

Capítulo 12 WANs punto a punto

Capítulo 13 Conceptos de Frame Relay

Capítulo 14 Configuración y resolución de problemas de Frame Relay

Capítulo 15 Redes privadas virtuales

Este capítulo trata los siguientes temas:

Conceptos de PPP: Esta sección examina los conceptos de PPP, incluyendo los protocolos de control y PAP/CHAP.

Configuración de PPP: Esta sección examina la forma de configurar un sencillo enlace PPP, así como la forma de configurar CHAP.

Resolución de problemas en enlaces serie: Esta sección examina el proceso general de resolución de problemas en enlaces serie, incluyendo las razones típicas por las que una interfaz tiene un determinado código de estado.

CAPÍTULO 12

WANs punto a punto

Este capítulo es el primero de los cuatro de que consta la Parte IV del libro. Esta parte se centra en las tecnologías WAN. El capítulo completa el estudio de los enlaces punto a punto, examinando más detalles relativos al funcionamiento de PPP, junto con una amplia gama de cuestiones de resolución de problemas relacionadas con las líneas punto a punto alquiladas. El Capítulo 13, "Conceptos de Frame Relay", y el Capítulo 14, "Configuración y resolución de problemas de Frame Relay", exploran las tecnologías de Frame Relay. El Capítulo 15, "Redes privadas virtuales", examina los conceptos que subyacen a las redes privadas virtuales (VPN). Las VPNs permiten crear rutas seguras de comunicaciones que se comportan como enlaces WAN cuando se utilizan otras redes menos seguras, como Internet.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las siete preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 12.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

Tabla 12.1. Relación entre las preguntas del cuestionario y los temas fundamentales del Capítulo.

Sección de Temas fundamentales	Preguntas
Conceptos de PPP	1 y 2
Configuración de PPP	3-5
Resolución de problemas en enlaces serie	6 y 7

1. ¿Cuál de los siguientes protocolos de autenticación PPP autentica al dispositivo situado en el otro extremo de un enlace sin enviar información de contraseña alguna en forma de texto plano?

a. MD5

b. PAP

c. CHAP

d. DES

2. ¿Cuál de los siguientes protocolos PPP controla el funcionamiento de CHAP?

a. CDPCP

b. IPCP

c. LCP

d. IPXCP

3. Dos routers carecen por completo de configuración inicial. Se conectan en un laboratorio empleando un cable DTE conectado a R1 y un cable DCE conectado a R2, y después los cables DTE y DCE se conectan entre sí. El ingeniero desea crear un enlace PPP operativo. ¿Cuáles de los comandos siguientes se requieren en R1 para que el enlace llegue a un estado en que R1 pueda hacer un ping a la dirección IP serie de R2, suponiendo que el enlace *bact-to-back* funciona físicamente?

a. encapsulation ppp

b. no encapsulation hdlc

c. clock rate

d. ip address

4. Imagine que dos routers, R1 y R2, tienen una línea alquilada que los une. Ambos routers han sufrido un borrado de su configuración, y después se han recargado. R1 ha sido configurado entonces con los siguientes comandos:

```
hostname R1
interface s0/0
 encapsulation ppp
 ppp authentication chap
```

¿Cuáles de los siguientes comandos de configuración pueden completar esta configuración en R1 para que CHAP pueda funcionar correctamente? Suponga que R2 se ha configurado correctamente y que la contraseña es fred.

a. No se necesita más configuración.

b. ppp chap (comando global).

c. username R1 password fred

d. username R2 password fred

e. ppp chap password fred

5. Considere el siguiente fragmento de la salida de un comando show:

```
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
```

```
Internet address is 192.168.2.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP
Open Open: CDPCP, IPCP, loopback not set
```

¿Cuáles de las afirmaciones siguientes, referidas a la interfaz S0/0/1 de este router, son verdaderas?

a. La interfaz utiliza HDLC.

b. La interfaz utiliza PPP.

c. En este momento la interfaz no admite tráfico IPv4.

d. El enlace debería admitir tramas PPP en este momento.

6. Considere el siguiente fragmento de la salida de un comando show interfaces aplicado a una interfaz que está configurada para emplear PPP:

```
Serial0/0/1 is up, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.168.2.1/24
```

Un ping de la dirección IP del otro extremo del enlace no tiene éxito. ¿Cuáles de las siguientes son causas del fallo, suponiendo que el problema indicado en esta respuesta fuera el único problema del enlace?

a. La CSU/DSU conectada al otro router no está encendida.

b. La dirección IP del router que está al otro extremo del enlace no está en la subred 192.168.2.0/24.

c. Ha fallado la autenticación CHAP.

d. El router que está al otro extremo del enlace se ha configurado para utilizar HDLC.

e. Ninguna de las otras respuestas es correcta.

7. Dos routers tienen un enlace serie que los une, y el enlace está configurado para utilizar PPP, con EIGRP configurado correctamente para todas las interfaces. El ingeniero puede hacer ping a la dirección IP del otro extremo del enlace, pero no a la dirección IP de la interfaz LAN del otro router. ¿Cuál de las siguientes respuestas es una causa probable del problema?

a. La CSU/DSU conectada al otro router no está encendida.

b. La dirección IP serie del router que está al otro extremo del enlace no está en la misma subred que el router local.

c. Ha fallado la autenticación CHAP.

d. El router que está al otro extremo del enlace se ha configurado para utilizar HDLC.

Temas fundamentales

El Protocolo punto a punto (PPP) define un protocolo de enlace de datos con muchas características, al margen de servir como ayuda para que dos dispositivos envíen datos a través del enlace. Este capítulo comienza explicando las muchas características de PPP que están disponibles en los routers, y después trata la configuración de PPP, incluyendo la configuración de la autenticación en PPP. El capítulo finaliza con una sección relativa a la resolución de problemas en enlaces serie, que abarca una amplia gama de temas, incluyendo PPP.

NOTA

Las opciones WAN, tales como las líneas alquiladas, la conmutación de paquetes y la CSU/DSU, así como un conocimiento básico de HDLC y de PPP, son requisitos previos para el examen ICND2 y para este libro. Sin embargo, si no dispone de una copia del libro **CCENT/CCNA ICND1**, el DVD de este libro contiene una copia del Capítulo 17 de ese libro como Apéndice I. Si todavía no ha leído el Capítulo 17 del libro ICND1, o si no tiene el libro, posiblemente sea este un buen momento para revisar el Apéndice I antes de seguir adelante con este capítulo.

Conceptos de PPP

PPP ofrece varias funciones básicas pero importantes que resultan útiles en líneas alquiladas que conectan dos dispositivos:

- Definición de una cabecera y una información final que permiten entregar tramas de datos a través del enlace.
- Soporte para enlaces tanto síncronos como asíncronos.
- Un campo de tipo de protocolo en la cabecera, que permite que múltiples protocolos de capa 3 pasen por el mismo enlace.
- Herramientas de autenticación incorporadas: Protocolo de autenticación de contraseña (PAP, *Password Authentication Protocol*) y Protocolo de autenticación de intercambio de señales por desafío (CHAP, *Challenge Handshake Authentication Protocol*).
- Protocolos de control para todos los protocolos de capas superiores que se basan en PPP, lo cual permite una integración y un soporte más fáciles para estos protocolos.

Las próximas páginas examinan con más detalle el campo de protocolo, la autenticación y los protocolos de control.

El campo de protocolo PPP

Una de las características más importantes que ofrece el estándar PPP, pero no el estándar HDLC, es el campo de protocolo. El campo de protocolo identifica el tipo de paquete

que se halla dentro de la trama. Cuando se creó PPP, este campo permitía que los paquetes de los muchos protocolos distintos de capa 3 pasaran a través de un único enlace. En la actualidad, el campo de tipo de protocolo sigue teniendo esa misma función, e incluso admite dos versiones diferentes de IP (IPv4 e IPv6). La Figura 12.1 compara los detalles de tramado de HDLC y PPP, y muestra el campo de protocolo exclusivo de HDLC y el campo de protocolo estandarizado de PPP.

Figura 12.1. Tramado de PPP y HDLC.

PPP define un conjunto de mensajes de control de capa 2 que llevan a cabo distintas funciones de control del enlace. Estas funciones de control pertenecen a dos categorías principales:

- Las que son necesarias independientemente del protocolo de capa 3 que se envíen a través del enlace.
- Las que son específicas de cada protocolo de capa 3.

El **Protocolo para el control del enlace** (*Link Control Protocol*, LCP) implementa las funciones de control que operan independientemente del protocolo de capa 3. Para las características relacionadas con protocolos de capas superiores, típicamente para los protocolos de capa 3, PPP utiliza una serie de **protocolos de control** (CP), tales como el Protocolo de control IP (IPCP). PPP utiliza un ejemplar de LCP por enlace, y un CP para cada protocolo de capa 3 que esté definido en el enlace. Por ejemplo, en un enlace PPP que utilice IPv4, IPv6 y el Protocolo de descubrimiento de Cisco (*Cisco Discovery Protocol*, CDP), el enlace emplea una instancia de LCP, y además IPCP (para IPv4), IPv6CP (para IPv6) y CDPCP (para CDP).

La sección siguiente resume las funciones de LCP y después explica una de esas funciones, la autenticación, con más detalle.

Protocolo para el control del enlace PPP (LCP)

LCP ofrece cuatro características notables, que se tratan en este capítulo. La Tabla 12.2 resume estas funciones, explica los nombres de las características de LCP y describe brevemente esas características. Después de la tabla, el texto explica las características con más detalle. Obsérvese que las características indicadas en la tabla son opcionales, y están inhabilitadas de forma predeterminada.

Tema clave **Tabla 12.2.** Características de LCP PPP.

Función	Característica de LCP	Descripción
Detección de enlaces con bucle	Número mágico	Detecta si el enlace contiene un bucle, y desactiva el enlace, permitiendo un nuevo enrutamiento a través de una ruta operativa.
Detección de errores	Monitorización de la calidad del enlace (*Link Quality Monitoring*, LQM)	Desactiva aquellas interfaces que exceden un cierto umbral de porcentaje de errores, permitiendo un nuevo enrutamiento a través de rutas mejores.
Soporte multienlace	PPP multienlace	Equilibra la carga de tráfico a través de múltiples enlaces paralelos.
Autenticación	PAP y CHAP	Intercambia nombres y contraseñas para que cada dispositivo pueda verificar la identidad del que se encuentra en el otro extremo del enlace.

Detección de enlaces con bucle

La detección de errores y la detección de enlaces en bucle son dos características fundamentales de PPP. La detección de enlaces en bucle permite una convergencia más rápida cuando falla un enlace a causa de un bucle. ¿Qué significa "en bucle"? Básicamente, para probar un circuito, la compañía de telefonía puede hacer que el circuito forme un bucle. El técnico se sienta en su puesto y, empleando comandos, hace que el switch de la compañía de telefonía forme un bucle en el circuito. Esto significa que la compañía de telefonía toma la señal eléctrica enviada por el dispositivo PE y devuelve la misma corriente eléctrica a ese mismo dispositivo.

Por supuesto, los routers no se pueden enviar bits entre sí mientras haya un bucle en el circuito. Sin embargo, ¡el router puede no apreciar que el enlace está embuclado, porque sigue recibiendo información a través del enlace! PPP ayuda al router a reconocer rápidamente los enlaces en bucle, para poder desactivar la interfaz y posiblemente para utilizar una ruta alternativa.

En algunos casos, la convergencia del protocolo de enrutamiento puede verse mejorada cuando LCP reconoce el bucle. Si el router puede observar inmediatamente que hay un bucle en un enlace, entonces puede poner la interfaz en el estado "*down*/*down*", y los protocolos de enrutamiento pueden modificar sus tablas de enrutamiento basándose en que ese enlace está desactivado. Si un router no aprecia que el enlace tiene un bucle, el protocolo de enrutamiento tiene que esperar a que se agoten los tiempos de espera; esto es, el router tiene que esperar a que pase un cierto tiempo sin tener noticias del router que se encuentra en el otro extremo del enlace.

LCP detecta rápidamente los enlaces en bucle por medio de una característica denominada **números mágicos**. Cuando utiliza PPP, el router envía a través del enlace mensajes LCP de PPP, en lugar de los *keepalives* de Cisco; estos mensajes contienen un número mágico que es distinto en cada router. Si una línea tiene un bucle, el router recibe un mensaje LCP con su propio número mágico, en lugar de recibir mensajes con el número mágico de algún otro router. Cuando un router recibe su propio número mágico, el router sabe que esa trama se le ha devuelvo a través de un bucle, así que puede desactivar la interfaz, lo cual acelera la convergencia.

Detección de errores mejorada

De forma similar a muchos otros protocolos de enlace de datos, PPP hace uso de un campo FCS en la información final de PPP para determinar si una determinada trama tiene un error. Si se recibe una trama con un error, la trama se descarta. Sin embargo, PPP puede monitorizar la frecuencia con que se reciben tramas con errores, para que pueda desactivar la interfaz si se producen demasiados errores.

LCP PPP analiza las tasas de error de los enlaces empleando una característica denominada Monitorización de la calidad del enlace (LQM). El LCP de los extremos del enlace envía mensajes que describen el número de paquetes y de bytes recibidos correctamente. El router que ha enviado los paquetes compara el número de tramas con error con el número de tramas y bytes enviados, y calcula el porcentaje de pérdidas. El router puede desactivar el enlace cuando se ha superado la tasa de errores especificada.

El único momento en que sirve de ayuda LQM es aquel en que se tienen rutas redundantes en la red. Al desactivar el enlace que tiene muchos errores, se puede hacer que los paquetes utilicen una ruta alternativa que quizá no tenga tantos errores.

Multienlace PPP

Cuando existen múltiples enlaces PPP entre dos routers (lo que se denomina enlaces paralelos), los routers tienen que determinar la forma de utilizar esos enlaces. Si se emplean enlaces HDLC, y enlaces PPP con la configuración más sencilla posible, los routers tienen que emplear un equilibrado de la carga de capa 3. Esto significa que los routers tienen múltiples rutas para las mismas subredes de destino. Por ejemplo, la parte superior de la Figura 12.2 muestra el efecto del equilibrado de la carga en R1 cuando se envían paquetes a la subred 192.168.3.0/24.

La figura muestra dos paquetes, uno de los cuales es grande y el otro pequeño. Empleando la lógica de capa 3, el router puede optar por enviar un paquete a través de un enlace, y el próximo a través de otro. Sin embargo, como los paquetes pueden ser de tamaños diferentes, quizá el router no equilibre igualmente el tráfico en todos los enlaces. En algunos casos, sobre todo cuando la mayoría de los paquetes se envía a unos pocos hosts de destino, el número de paquetes enviados por cada enlace puede no estar equilibrado, lo cual podría hacer que un enlace estuviera sobrecargado mientras otro está desocupado.

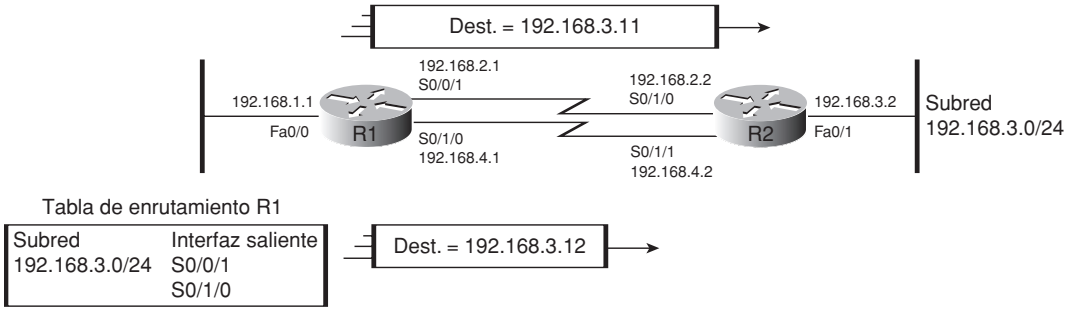


Figura 12.2. Equilibrado de la carga sin PPP multienlace.

El multienlace PPP equilibra la carga de tráfico por igual a través de los enlaces, y además permite a la lógica de capa 3 de los routers tratar a los enlaces paralelos como si fuesen un único enlace. Cuando se encapsula un paquete, PPP fragmenta el paquete en tramas más pequeñas, y envía un fragmento a través de cada enlace. Por ejemplo, para la red que se muestra en la Figura 12.2, y que posee dos enlaces, R1 crearía dos tramas por cada paquete de capa 3, y cada trama contendría aproximadamente la mitad del paquete original. Entonces PPP envía un fragmento de cada paquete original a través de cada uno de los dos enlaces. Al enviar aproximadamente medio paquete a través de cada enlace, PPP multienlace puede efectuar un equilibrado de la carga más igualado. Como beneficio adicional, PPP permite que las tablas de enrutamiento de capa 3 utilicen una sola ruta que hace alusión a los enlaces combinados, reduciendo el tamaño de la tabla de enrutamiento. Por ejemplo, en la Figura 12.2, R1 utilizaría una sola ruta para la subred 192.168.3.0/24, y denotaría el grupo de interfaces como un concepto que recibe el nombre de **grupo multienlace**.

Autenticación en PPP

El término **autenticación** denota una colección de funciones de seguridad que sirven de ayuda para que un dispositivo confirme que el otro dispositivo debe recibir permiso para comunicarse, y no es un impostor. Por ejemplo, si R1 y R2 se estuvieran comunicando a través de un enlace serie, R1 podría desear que R2 demostrase de algún modo que realmente es R2. La autenticación es una forma de demostrar la propia identidad.

La autenticación WAN se precisa con especial frecuencia cuando se emplean líneas de marcación telefónica. Sin embargo, la configuración de las características de autenticación sigue siendo la misma tanto si se emplea una línea alquilada como una línea de marcación telefónica.

PAP y CHAP comprueban la autenticidad de ambos extremos en enlaces serie punto a punto. CHAP es el método preferido en la actualidad, porque el proceso de identificación utiliza valores ocultos con un compendio de mensaje 5 (MD5) unidireccional, que es más seguro que las contraseñas en texto puro que envía PAP.

Tanto PAP como CHAP requieren un intercambio de mensajes entre dispositivos. Cuando se utiliza una línea telefónica, el router de destino espera recibir un nombre de usuario y

una contraseña procedentes del router que hace la llamada, tanto en el caso de PAP como en el de CHAP. Cuando se utiliza una línea alquilada, lo típico es que ambos routers se autentiquen entre sí. Tanto en una línea alquilada como en una línea telefónica, si se emplea PAP entonces el nombre de usuario y la contraseña se envían en el primer mensaje. Si se utiliza CHAP, el protocolo comienza por un mensaje que se denomina *challenge* (intercambio de señales por desafío), que pide al otro router que envíe su nombre de usuario y su contraseña. La Figura 12.3 muestra los distintos procesos del caso en que los enlaces son de línea telefónica. El proceso funciona de igual modo cuando el enlace hace uso de una línea alquilada.

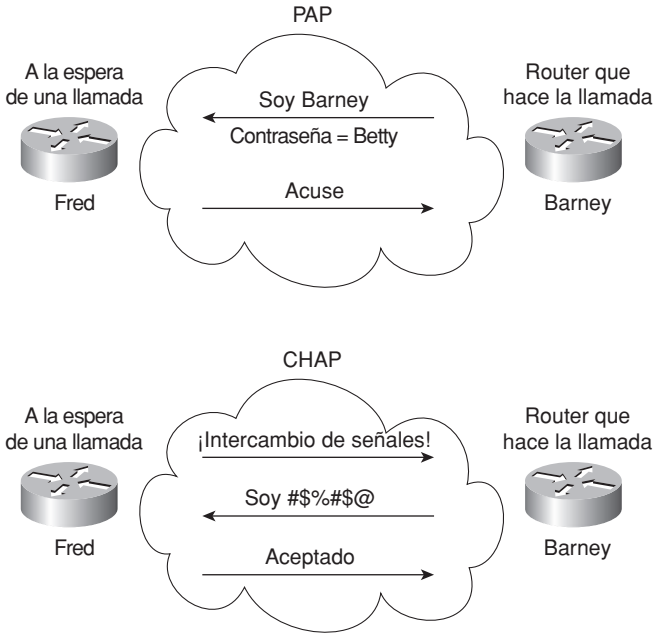


Figura 12.3. Proceso de autenticación en PAP y CHAP.

Los flujos PAP son mucho menos seguros que los basados en CHAP, porque PAP envía el nombre de usuario y la contraseña en texto sin formato dentro del mensaje. Esta información se puede leer fácilmente si alguien pone una herramienta de rastreo en el circuito. Por su parte, CHAP utiliza un algoritmo *hash* unidireccional, en el cual la entrada al algoritmo es una contraseña que nunca pasa por el enlace, más un número aleatorio compartido. El intercambio de señales por desafío de CHAP indica el número aleatorio; ambos routers han sido configurados previamente con la contraseña. El router de destino ejecuta el algoritmo *hash* empleando el número aleatorio que acaba de conocer y la contraseña secreta, y devuelve los resultados al router que ha enviado la petición. El router que envió la petición ejecuta el mismo algoritmo empleando el número aleatorio (que se ha enviado a través del enlace) y la contraseña (que no se envía a través del enlace). Si coinciden los resultados, las contraseñas tienen que coincidir.

La parte más interesante del proceso CHAP es que la contraseña nunca llega a pasar por el enlace. Con el número aleatorio, el valor obtenido por dispersión (*hash*) es distinto en todas las ocasiones. Por tanto, aunque alguien vea el valor *hash* calculado empleando una herramienta de rastreo, el valor carece de sentido para intentar descifrar el mensaje la próxima vez. La autenticación CHAP es difícil de superar, aunque se tenga una herramienta de rastreo en el enlace WAN.

Configuración de PPP

Esta sección examina la forma de configurar PPP y después la forma de añadir la configuración de CHAP. Además, se examinan también dos comandos que ayudan a verificar si PPP está activado y en funcionamiento.

Configuración básica de PPP

La configuración de PPP sólo requiere ejecutar el comando encapsulation ppp en ambos extremos del enlace. Para volver a utilizar el valor predeterminado de HDLC, el ingeniero solo necesita volver a utilizar el comando encapsulation hdlc en ambos extremos del enlace. Sin embargo, además de esta configuración básica, el enlace serie físico tiene que ser solicitado e instalado. Esta sección supone que el enlace físico ya está instalado y está funcionando. Si desea leer más detalles respecto al enlace físico, consulte el Capítulo 17 del libro **CCENT/CCNA ICND1**, o la copia de ese capítulo que se incluye en el Apéndice I de este libro (y que sólo está disponible en el DVD).

El Ejemplo 12.1 muestra una sencilla configuración que hace uso de los dos routers que se muestran en la Figura 12.4. El ejemplo incluye la configuración de la dirección IP, pero no es preciso configurar las direcciones IP para que funcione PPP. Como la mayoría de las instalaciones van a utilizar IP, se añade la configuración para dar una idea de los comandos show que hay en la segunda parte del ejemplo.

Ejemplo 12.1. Configuración básica de PPP.

```
! El ejemplo empieza con el router R1
interface Serial0/0/1
 ip address 192.168.2.1 255.255.255.0
 encapsulation ppp
 clockrate 1536000
! A continuación, la configuración en el router R2
interface Serial0/1/1
 ip address 192.168.2.2 255.255.255.0
 encapsulation ppp
! De nuevo en el router R1
```

(continúa)

Ejemplo 12.1. Configuración básica de PPP *(continuación).*

```
R1#show interfaces serial 0/0/1
Serial0/0/1 is up, line protocol is up
 Hardware is GT96K Serial
 Internet address is 192.168.2.1/24
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation PPP, LCP Open
 Open: CDPCP, IPCP, loopback not set
! Se han omitido algunas líneas por brevedad
```

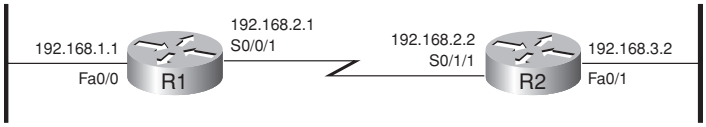


Figura 12.4. Red con dos routers que se utiliza en los ejemplos de PPP.

Este ejemplo muestra la configuración sencilla, en la que ambos routers precisan utilizar el encapsulamiento PPP. Si alguno de los routers tomara el valor predeterminado, que es HDLC, y el otro configurase PPP como se muestra, el enlace no se activaría, y la interfaz permanecería en un estado "*up*/*down*".

El comando show interfaces que hay en la parte inferior del ejemplo muestra el resultado normal cuando el enlace está activado y en funcionamiento. El segundo código de estado se refiere típicamente al estado del enlace de datos, donde el valor "*up*" significa que el enlace de datos está en funcionamiento. Adicionalmente, las frases que se han resaltado muestran que realmente está configurado PPP, y que LCP ya ha finalizado su tarea con éxito, según indica la frase "LCP Open". Por otra parte, el resultado muestra que los dos CPs, CDPCP e IPPCP, también se han habilitado con éxito; todo esto son buenas indicaciones de que PPP está funcionando correctamente.

Configuración y verificación de CHAP

La versión más sencilla de la configuración de CHAP sólo requiere unos pocos comandos. La configuración hace uso de una contraseña que se configura en ambos routers. Como alternativa, se podría configurar la contraseña en un servidor externo de Autenticación, autorización y auditoría (AAA) situado fuera del router. Los pasos de configuración son como sigue:

Paso 1 Configurar los nombres de los routers empleando el comando global de configuración hostname *nombre*.

Tema clave

Paso 2 Configurar el nombre del otro router, y la contraseña secreta compartida, empleando el comando global de configuración username *nombre* password *contraseña*.

Paso 3 Habilitar CHAP en la interfaz de ambos routers, empleando el subcomando de interfaz ppp authentication chap.

El Ejemplo 12.2 muestra un ejemplo de configuración, empleando los dos routers del ejemplo anterior (véase la Figura 12.4).

Ejemplo 12.2. Ejemplo de configuración de CHAP.

```
hostname R1

username R2 password mypass
!
interface serial 0/0/1
 encapsulation ppp
 ppp authentication chap
```

```
hostname R2

username R1 password mypass
!
interface serial 0/1/1
 encapsulation ppp
 ppp authentication chap
```

Los comandos en sí no son complicados, pero es fácil configurar incorrectamente los nombres y las contraseñas de los routers. Obsérvese que cada router se refiere al nombre de host del otro en el comando username, pero es preciso configurar ambos routers con la misma contraseña. Además, en las contraseñas (que en este caso es mypass) se distingue entre mayúsculas y minúsculas; y también en los nombres de host, a los que se hace alusión en el comando username.

Como CHAP es una función de LCP, si falla el proceso de autenticación, entonces LCP no finaliza, y la interfaz cae en un estado "*up*/*down*".

Configuración de PAP

PAP utiliza exactamente los mismos comandos de configuración que CHAP, salvo que se emplea el comando ppp authentication pap en lugar de ppp authentication chap. Los demás comandos de verificación funcionan igual, independientemente de cual de los dos tipos de autenticación se utilice. Por ejemplo, si falla la autenticación PAP, entonces falla LCP y el enlace cae en un estado "*up*/*down*".

El software IOS de Cisco admite también la posibilidad de configurar el router de tal modo que primero pruebe un método de autenticación y, si el otro lado no contesta, pruebe después la otra opción. Por ejemplo, el subcomando de interfaz ppp authentication chap pap indica al router que envíe mensajes CHAP; si no recibe respuesta, debe probar con PAP. Obsérvese que la segunda opción no se llega a probar si fluyen mensajes CHAP entre ambos dispositivos, y el resultado es que falla la autenticación. Se utiliza la otra opción únicamente si el otro dispositivo no devuelve mensaje alguno.

La sección siguiente muestra una amplia gama de temas relacionados con la resolución de problemas WAN, incluyendo algunos detalles más relativos a la resolución de problemas en CHAP.

Resolución de problemas en enlaces serie

Esta sección describe la forma de aislar y buscar la causa raíz de problemas relacionados con temas que se han tratado anteriormente en este capítulo, y también algunos temas relativos a redes WAN punto a punto que se tratan en el libro **CCENT/CCNA ICND1**. Además, esta sección no intenta repetir los temas de resolución de problemas de IP que hay en las Partes II y III del libro, aunque ciertamente señala algunos de los posibles síntomas de un enlace serie cuando se produce una desigualdad de subred en la capa 3 en extremos opuestos de un enlace serie, lo cual impide a los routers enrutar paquetes a través del enlace serie.

Un sencillo comando ping puede determinar si un enlace serie puede o no enviar paquetes IP. Un ping de la dirección IP serie del otro router (por ejemplo, un comando ping 192.168.2.2 en R1, en la Figura 12.4) demuestra si el enlace funciona o no.

Si no funciona el ping, el problema podría estar relacionado con funciones de las capas 1, 2 ó 3. La mejor manera de aislar qué capa es la que con más probabilidad causa el problema consiste en examinar los códigos de estado de la interfaz que se describen en la Tabla 12.3. (Como recordatorio, las interfaces de un router tienen dos códigos de estado: un estado de línea y un estado de protocolo.)

Tabla 12.3. Códigos de estado de la interfaz y su posible significado cuando no funciona un ping.

Estado de línea	Estado de protocolo	Razón/capa probable
Administrativamente *down*	*Down*	Interfaz cerrada
Down	*Down*	Capa 1
Up	*Down*	Capa 2
Up	*Up*	Capa 3

El proceso de resolución de problemas y verificación en enlaces serie debería comenzar con un sencillo proceso de tres pasos:

Paso 1 Desde un router, se hace un ping a la dirección IP serie del otro router.

Paso 2 Si falla el ping, se examina el estado de la interfaz en ambos routers, y se investigan los problemas relacionados con los aspectos problemáticos que se enumeran en la Tabla 12.4 (que se muestra más adelante en este capítulo).

Paso 3 Si funciona el ping, se verifica también que los posibles protocolos de enrutamiento están realmente intercambiando rutas a través del enlace.

Nota

Los códigos de estado de la interfaz se pueden obtener empleando los comandos show interfaces, show ip interface brief y show interfaces description.

El resto del capítulo trata los temas concretos que deben examinarse cuando falla el ping, basándose en las combinaciones de códigos de estado de interfaz que se muestran en la Tabla 12.3.

Resolución de problemas de capa 1

Los códigos de estado de interfaz, o estado de la interfaz, desempeñan un papel clave a la hora de aislar la causa raíz de los problemas que aparecen en los enlaces serie. De hecho, el estado de ambos extremos del enlace puede diferir, así que es importante examinar el estado de ambos extremos del enlace para intentar determinar el problema.

Existe un problema de capa 1 que resulta sencillo y fácil de hallar, y se produce cuando cualquiera de los dos routers ha desactivado administrativamente su interfaz serie mediante el subcomando de interfaz shutdown. Si la interfaz serie de un router está en un estado de línea desactivado administrativamente, la solución es sencilla: se aplica un comando de configuración de interfaz no shutdown a esta interfaz. Además, si la interfaz de un router tiene un estado de línea desactivado, el otro router puede estar apagado, así que hay que comprobar ambos lados del enlace.

La combinación del estado de línea *down* en ambos extremos de un enlace serie denota un problema de capa 1. La lista siguiente describe las razones más probables:

Tema clave

- La línea alquilada no funciona (un problema del proveedor de la línea).
- La línea del proveedor no está conectada a alguna de las CSU/DSUs o a las dos.
- Hay una CSU/DSU que ha fallado o no está bien configurada.
- Hay un cable serie de un router a su CSU/DSU que está desconectado o ha fallado.

Los detalles relativos a la forma de aislar aún más estos cuatro problemas van más allá del alcance de este libro.

Curiosamente, hay un problema frecuente de la capa física que puede dar lugar a que las interfaces de ambos routers se encuentren en un estado *up*/*down*. En un enlace serie *back-to-back*, si falta el comando clock rate requerido en el router que tiene instalado un cable DCE, entonces las interfaces serie de ambos routers fallarán y tendrán un estado de línea "*up*" pero un estado de protocolo "*down*". El Ejemplo 12.3 muestra uno de estos ejemplos, e indica un par de formas de comprobar si el problema es que falta un comando clock rate. Las dos mejores maneras de detectar este problema consisten en notar la ausencia del comando clock rate en el router que tiene el cable DCE, y observar la frase "no clock" en la salida del comando show controllers serial. (Este ejemplo muestra a R1, de la Figura 12.4, en el que se ha eliminado el comando clock rate.)

Nota

Algunas versiones recientes del IOS llegan a impedir que el usuario borre el comando clock rate de la interfaz si hay un cable DCE conectado o si no se ha instalado cable alguno, intentando evitar la omisión no intencionada del comando clock rate. Además, en ciertas ocasiones el IOS acepta el comando clock rate en la forma clockrate; se admiten las dos formas.

Ejemplo 12.3. Problema: no existe el comando **clock rate** en el extremo que tiene el DCE.

```
R1#show controller s0/0/1
Interface Serial0/0/1
Hardware is PowerQUICC MPC860
  Internet address is 192.168.2.1/24
DCE V.35, no clock
! Se omiten líneas para abreviar
R1#show running-config interface S0/0/1
Building configuration...

Current configuration : 42 bytes
!
interface Serial0/0/1
 ip address 192.168.2.1 255.255.255.0
end
```

Resolución de problemas de capa 2

Cuando el estado de la línea serie de ambos routers es "*up*", pero el estado de protocolo de al menos una de las líneas del router (el segundo código de estado de la interfaz) es "*down*", o cambia continuamente entre "*up*" y "*down*", es probable que la interfaz tenga uno de los dos tipos de problemas de la capa de enlace de datos. Esta sección explica los dos problemas, que se han resumido en la Tabla 12.4.

Tabla 12.4. Razones probables de los problemas de enlace de datos en los enlaces serie.

Estado de línea	Estado de protocolo	Razón/capa probable
Up	*Down* (estable) en los dos extremos o bien *Down* (estable) en un extremo, cambiando entre *up* y *down* en el otro	Comandos encapsulation no coincidentes
Up	*Down* en un extremo, *up* en el otro	*Keepalive* deshabilitado en el extremo con estado *up*
Up	*Down* (estable) en los dos extremos	Fallo en la autenticación PAP/CHAP

NOTA

Tal como se ha hecho en los demás temas de resolución de problemas de este libro, la Tabla 12.4 enumera algunos de los tipos de fallos más comunes, pero no todos.

El primero de estos dos problemas (una desigualdad entre los protocolos configurados para el enlace de datos) resulta fácil de identificar y de corregir. El comando show interfaces muestra el tipo de encapsulamiento en la séptima línea de la salida, así que al utilizar este comando en ambos routers se puede identificar rápidamente el problema. Alternativamente, un rápido examen de la configuración, recordando que el encapsulamiento serie predeterminado es HDLC, puede confirmar si los encapsulamientos son o no desiguales. La solución es sencilla: reconfigurar los dos routers para que coincidan sus comandos encapsulation.

Las otras dos causas principales requieren un poquito más de explicación para comprender el problema y determinar si son realmente la causa principal. Las dos secciones siguientes examinan con más detalle los dos problemas.

Fallo de *keepalive*

La segunda cuestión está relacionada con una característica denominada *keepalive*. Esta característica ayuda al router a darse cuenta de que un enlace ya no funciona, para que el router pueda desactivar la interfaz correspondiente, con la intención de utilizar una ruta IP alternativa.

La función *keepalive* (de modo predeterminado) hace que los routers vayan enviándose entre sí mensajes de actividad (*keepalive*) cada 10 segundos (este es el ajuste predeterminado). (Cisco define un mensaje de actividad HDLC exclusivo, y PPP define un mensaje de actividad que forma parte de LCP.) Este temporizador de 10 segundos es el intervalo activo. Si un router no recibe ningún mensaje de actividad procedente del otro router durante un cierto número de intervalos activos (tres o cinco intervalos de modo predeterminado, dependiendo de la versión del IOS), entonces el router desactiva la interfaz, pensando que esa interfaz ya no funciona.

Para las redes reales resulta útil dejar activados los intervalos activos. Sin embargo, se puede cometer un error y desactivarlos en un extremo de un enlace serie, dejándolos activados en el otro; esto dará lugar a que falle el enlace. Por ejemplo, si R1 se configurase con el subcomando de interfaz no keepalive, que desactiva los intervalos activos, entonces R1 ya no enviaría mensajes de actividad. Si R2 siguiera empleando el método predeterminado, consistente en emplear mensajes de actividad, R2 seguiría enviándolos, y además R2 esperaría recibirlos procedentes de R1. Una vez transcurridos varios intervalos activos, R2, que no habría recibido ningún mensaje de actividad procedente de R1, haría que la interfaz pasase al estado "*up*/*down*". Entonces R2 volvería a activar continuamente el enlace, no recibiría mensajes de actividad de R1 y volvería a caer en un estado "*up*/*down*" una vez más, y seguiría activando y desactivando la interfaz indefinidamente. R1, que no se preocupa por los mensajes de actividad, dejaría la interfaz en el estado "*up*/*up*" indefinidamente. El Ejemplo 12.4 muestra exactamente esta situación, empleando una vez más los routers de la Figura 12.4.

Ejemplo 12.4. Problemas de línea porque el intervalo activo sólo está activado en R2.

```
! R1 inhabilita los intervalos activos y permanece en estado up/up
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface s 0/0/1
R1(config-if)#no keepalive
R1(config-if)#^Z
R1#show interfaces s0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 192.168.2.1/24 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive not set
! Se han omitido ciertas líneas por brevedad
! A continuación, R2 todavía tiene los keepalives activados (lo predeterminado)
R2#show interfaces S0/1/1
Serial0/1/1 is up, line protocol is down
  Hardware is PowerQUICC Serial
  Internet address is 192.168.2.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
! Se han omitido ciertas líneas por brevedad
```

Nota

Es un error de configuración activar los intervalos activos en un solo extremo de un enlace serie punto a punto. Parece que ciertas versiones muy recientes del IOS perciben cuándo estos mensajes están desactivados (incorrectamente) en un extremo del enlace, y evitan el problema descrito aquí. Para los exámenes de CCNA, basta tener en cuenta que estos mensajes deberían estar activados en ambos extremos del enlace, o bien desactivados en ambos.

Fallos de autenticación en PAP y CHAP

Según lo indicado anteriormente, un fallo en el proceso de autenticación PAP/CHAP da lugar a que ambos routers caigan en un estado "*up/down*". Para descubrir si la causa inicial es realmente un fallo de PAP/CHAP, se puede utilizar el comando debug ppp authentication. Como caso estudio, el Ejemplo 12.5 muestra la salida de este comando cuando se ha configurado CHAP como en el Ejemplo 12.2 anterior, pero con CHAP funcionando correctamente en este caso.

Ejemplo 12.5. Mensajes de depuración que confirman el correcto funcionamiento de CHAP.

```
R1#debug ppp authentication
PPP authentication debugging is on
R1#
*May 21 18:26:55.731: Se0/0/1 PPP: Using default call direction
*May 21 18:26:55.731: Se0/0/1 PPP: Treating connection as a dedicated line
*May 21 18:26:55.731: Se0/0/1 PPP: Authorization required
*May 21 18:26:55.731: Se0/0/1 CHAP: O CHALLENGE id 16 len 23 from "R1"
*May 21 18:26:55.731: Se0/0/1 CHAP: I CHALLENGE id 49 len 23 from "R2"
*May 21 18:26:55.735: Se0/0/1 CHAP: Using hostname from unknown source
*May 21 18:26:55.735: Se0/0/1 CHAP: Using password from AAA
*May 21 18:26:55.735: Se0/0/1 CHAP: O RESPONSE id 49 len 23 from "R1"
*May 21 18:26:55.735: Se0/0/1 CHAP: I RESPONSE id 16 len 23 from "R2"
*May 21 18:26:55.735: Se0/0/1 PPP: Sent CHAP LOGIN Request
*May 21 18:26:55.735: Se0/0/1 PPP: Received LOGIN Response PASS
*May 21 18:26:55.735: Se0/0/1 PPP: Sent LCP AUTHOR Request
*May 21 18:26:55.735: Se0/0/1 PPP: Sent IPCP AUTHOR Request
*May 21 18:26:55.735: Se0/0/1 LCP: Received AAA AUTHOR Response PASS
*May 21 18:26:55.739: Se0/0/1 IPCP: Received AAA AUTHOR Response PASS
*May 21 18:26:55.739: Se0/0/1 CHAP: O SUCCESS id 16 len 4
*May 21 18:26:55.739: Se0/0/1 CHAP: I SUCCESS id 49 len 4
```

CHAP emplea un intercambio de tres mensajes, según se mostraba anteriormente en la Figura 12.3, con un conjunto de mensajes que se envían en ambas direcciones para realizar la autenticación de forma predeterminada. Las tres líneas que están resaltadas muestran el proceso de autenticación mediante el que R1 reconoce como válido a R2; comienza con R1 que envía un mensaje de intercambio de señales. El primer mensaje marcado en el Ejemplo 12.5 muestra una "O", que significa "*output* (salida)". Esto indica que el mensaje es un mensaje de intercambio de señales y se ha enviado desde R1. El próximo mensaje marcado es el mensaje recibido como respuesta (que se denota con una "I" de *input* [entrada]), procedente de R2. La última línea marcada es el tercer mensaje, enviado por R1, que indica que la autenticación ha tenido éxito. También se pueden ver los tres mensajes mediante los cuales R2 reconoce a R1 en la salida, pero no se han marcado esos mensajes en el ejemplo.

Cuando falla la autenticación CHAP, el resultado de debug muestra un par de mensajes bastante evidentes. El Ejemplo 12.6 muestra los resultados empleando la misma red de dos routers que se muestra en la Figura 12.4, pero esta vez con las contraseñas mal configuradas, así que CHAP falla.

Ejemplo 12.6. Mensajes de depuración que confirman que CHAP ha fallado.

```
R1#debug ppp authentication
PPP authentication debugging is on
! Se han omitido ciertas líneas por brevedad
*May 21 18:24:03.171: Se0/0/1 PPP: Sent CHAP LOGIN Request
*May 21 18:24:03.171: Se0/0/1 PPP: Received LOGIN Response FAIL
*May 21 18:24:03.171: Se0/0/1 CHAP: O FAILURE id 15 len msg is "Authentication
                                    failed"
```

Resolución de problemas de capa 3

Este capítulo sugiere que el mejor punto de partida para la resolución de problemas en enlaces serie consiste en hacer un ping a la dirección IP del router que haya en el otro extremo del enlace; concretamente, debe hacerse un ping a la dirección IP del enlace serie. Curiosamente, el enlace serie puede hallarse en un estado "*up*/*up*" y producir un fallo en el ping como consecuencia de una configuración incorrecta de la capa 3. En algunos casos el ping puede funcionar, pero los protocolos de enrutamiento quizá no puedan intercambiar rutas. Esta breve sección examina los síntomas, que son ligeramente distintos dependiendo de si se emplea HDLC o PPP, y de la causa raíz.

En primer lugar, considere un enlace HDLC en el que los detalles físicos y de enlace de datos estén funcionando perfectamente. En este caso, las interfaces de los dos routers se hallarán en el estado "*up*/*up*". Sin embargo, si la dirección IP configurada en las interfaces serie de ambos routers se hallan en distintas subredes, un ping a la dirección IP del otro extremo del enlace fallará, porque los routers no tienen una ruta coincidente. Por ejemplo, en la Figura 12.4, si la dirección IP de R1 siguiera siendo 192.168.2.1, y la de R2 cambiara a 192.168.3.2 (en lugar de ser 192.168.2.2), manteniendo la máscara /24, entonces los dos routers tendrían rutas conectadas a subredes diferentes. No tienen una ruta que coincida con la dirección IP serie del router contrario.

La búsqueda y corrección de un problema de subred desigual en enlaces HDLC son relativamente sencillas. Se puede observar el problema efectuando el primer paso habitual, consistente en hacer un ping a la dirección IP del otro extremo del enlace, produciéndose un fallo. Si los códigos de estado de interfaz de ambos routers son "*up*", es probable que el problema sea esta subred con IP desigual.

Para los enlaces PPP, con los mismos errores de configuración respecto a la dirección IP y a la máscara, las interfaces de ambos routers también están en el estado "*up*/*up*", pero un ping a la dirección IP del otro router sí va a funcionar. Lo que sucede es que los routers que utilizan PPP publican la dirección IP de su interfaz serie al otro router, con el prefijo /32, que es una ruta para llegar tan sólo a ese dispositivo. Por tanto, ambos routers tienen una ruta mediante la cual pueden enrutar paquetes al otro extremo del enlace, aun cuando los routers de extremos opuestos de un enlace serie estén configurados con direcciones IP que no coincidan. Por ejemplo, de nuevo en la Figura 12.4, si la dirección IP de R2 fuera 192.168.4.2/24, y la de R1 siguiera siendo 192.168.2.1/24, las dos direcciones se hallarían en subredes diferentes, pero los *pings* funcionarían porque PPP notifica las rutas de los dos dispositivos. El Ejemplo 12.7 muestra exactamente esta situación.

Nota

Una ruta con el prefijo /32, que representa a un único dispositivo, se denomina **ruta de host**.

La primera línea resaltada en el ejemplo muestra la ruta normal conectada al enlace serie, para la red 192.168.2.0/24. R1 piensa que esta subred es la subred conectada a S0/0/1 por la dirección IP configurada en R1 (192.168.2.1/24). La segunda línea resaltada

Ejemplo 12.7. PPP permite hacer ping a través de un enlace serie, aunque no coincidan las subredes.

```
R1#show ip route
Codes:  C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

C     192.168.1.0/24 is directly connected, FastEthernet0/0
C     192.168.2.0/24 is directly connected, Serial0/0/1
      192.168.4.0/32 is subnetted, 1 subnets
C     192.168.4.2 is directly connected, Serial0/0/1
R1#ping 192.168.4.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

muestra la ruta de host creada por PPP, específicamente para la nueva dirección IP serie de R2 (192.168.4.2). (R2 tendrá una ruta parecida para la dirección IP serie de R1, que es 192.168.2.1/32.) Por tanto, ambos routers tienen una ruta que les permite reenviar paquetes a la dirección IP del otro extremo del enlace, lo cual permite que funcione un ping hacia el otro lado del enlace serie a pesar de que las direcciones de los extremos se encuentren en subredes diferentes.

Aunque el ping del otro extremo del enlace funciona, los protocolos de enrutamiento siguen sin publicar sus rutas como consecuencia de la desigualdad de subredes IP que afecta a los extremos opuestos del enlace. Por tanto, cuando se resuelven problemas de redes, no se puede suponer que una interfaz serie que se halle en el estado *up*/*up* es totalmente operativa. También hay que asegurarse de que el protocolo de enrutamiento está intercambiando rutas y de que las direcciones IP se encuentran en la misma subred. La Tabla 12.5 resume el comportamiento en enlaces HDLC y PPP cuando las direcciones IP de los extremos no residen en la misma subred, pero no hay otros problemas.

Tabla 12.5. Resumen de síntomas en caso de desigualdad de subred en enlaces serie.

Síntomas cuando las direcciones IP en un enlace serie están en subredes diferentes	**HDLC**	**PPP**
¿Funciona un ping de la dirección IP serie del otro router?	No	Sí
¿Los protocolos de enrutamiento pueden intercambiar rutas a través del enlace?	No	No

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 12.6 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 12.6. Temas clave del Capítulo 12.

Tema clave	Descripción	Número de página
Lista	Caraterísticas de PPP	440
Tabla 12.2	Características de LCP en PP	442
Figura 12.3	Comparación de los mensajes que envía PAP y CHAP	445
Lista	Lista de comprobación para la configuración de CHAP	447-448
Tabla 12.3	Lista de combinaciones típicas de códigos de estado en interfaces serie, y razón típica general para cada combinación	449
Lista	Razones comunes para problemas de enlaces de la Capa 1	450
Tabla 12.4	2 problemas de los enlaces serie	451
Ejemplo 12.5	Ejemplos de mensajes **debug** que muestran un proceso de autentificación CHAP que tiene éxito	454

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Tablas de memorización" (disponible en el DVD), o al menos de la sección correspondiente a este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización" también disponible en el DVD, contiene las tablas y las listas completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe sus respuestas en el glosario:

CHAP, PAP, protocolo de control del enlace, protocolo de control IP.

Referencias de comandos

Aunque no necesariamente debe memorizar la información de las tablas de esta sección, ésta incluye una referencia de los comandos de configuración y EXEC utilizados en este capítulo. En la práctica, debería memorizar los comandos como un efecto colateral de leer el capítulo y hacer todas las actividades de esta sección de preparación del examen. Para verificar si ha memorizado los comandos como un efecto colateral de sus otros estudios, cubra el lado izquierdo de la tabla con un trozo de papel, lea las descripciones del lado derecho y compruebe si recuerda el comando.

Tabla 12.7. Comandos de configuración del Capítulo 12.

Comando	Descripción
encapsulation {hdlc | ppp}	Subcomando de interfaz que define el protocolo de enlace de datos serie.
ppp authentication {pap | chap | pap chap | chap pap}	Subcomando de interfaz que habilita únicamente PAP, o CHAP, o ambos (dependiendo de la orden).
username *nombre* password *secreto*	Comando global que establece la contraseña que espera utilizar este router cuando autentique al router cuyo nombre de host se indica.

Tabla 12.8. Comandos EXEC del Capítulo 12.

Comando	Descripción
show interfaces [*tipo número*]	Muestra estadísticas y detalles de la configuración de la interfaz, incluyendo el tipo de encapsulamiento.
debug ppp authentication	Genera mensajes para cada paso del proceso de autenticación PAP o CHAP.
debug ppp negotiation	Genera mensajes debug para los mensajes de negociación LCP y NCP intercambiados entre dos dispositivos.

Este capítulo trata los siguientes temas:

Visión general de Frame Relay: Esta sección presenta la terminología, las funciones y el propósito de los protocolos de Frame Relay.

Direccionamiento en Frame Relay: Esta sección examina el DLCI, la dirección de enlace de datos de Frame Relay, y la forma en que se utiliza para transferir tramas a través de la nube de Frame Relay.

Temas de la capa de red relativos a Frame Relay: Esta sección examina principalmente las distintas opciones asociadas al uso de subredes de la capa 3 a través de una red Frame Relay.

Control de la velocidad y de los descartes en la nube Frame Relay: Esta sección, más bien breve, explica algunos detalles relativos al control del flujo de datos a través de la red Frame Relay.

CAPÍTULO 13

Conceptos de Frame Relay

Frame Relay sigue siendo la tecnología WAN más difundida en la actualidad. Sin embargo, su popularidad está en declive. Está siendo reemplazada principalmente por la tecnología de redes privadas virtuales (VPN) de dos tipos principales: VPN Internet, que hace uso de Internet para transportar paquetes, y VPN basada en la Conmutación multiprotocolo por etiquetas (*Multiprotocol Label Switching*, MPLS), que siguen el mismo modelo básico de servicio que Frame Relay, y son ofrecidas típicamente por los mismos proveedores que Frame Relay, pero con ventajas técnicas significativas. Sin embargo, en la actualidad muchas compañías siguen utilizando Frame Relay, y también se puede utilizar para establecer conexiones con las VPNs MPLS e Internet, así que Frame Relay seguirá siendo un tema importante en el mundo de las redes durante un cierto tiempo.

Frame Relay se parece especialmente a la capa de datos de ISO (capa 2). Si recordamos que la palabra "frame" (trama) denota la unidad de datos del protocolo de la capa de enlace de datos (PDU), será fácil recordar que Frame Relay está relacionado con la capa 2 de ISO. Al igual que otros protocolos de enlace de datos, Frame Relay se puede usar para entregar paquetes (PDU de la capa 3) entre routers. Las cabeceras y las informaciones finales del protocolo de Frame Relay se utilizan para permitir que el paquete recorra la red de Frame Relay, del mismo modo que las cabeceras y las informaciones finales de Ethernet sirven para ayudar a que el paquete recorra segmentos de Ethernet.

Este capítulo describe los detalles del protocolo Frame Relay. El Capítulo 14, "Configuración y resolución de problemas de Frame Relay", examina la configuración, verificación y resolución de problemas en redes Frame Relay.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las ocho preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 13.1 especifica

Tabla 13.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
Visión general de Frame Relay	1-3
Direccionamiento en Frame Relay	4 y 5
Temas de la capa de red relativos a Frame Relay	6 y 7
Control de la velocidad y de los rechazos en la nube Frame Relay	8

los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

1. ¿Cuál de los siguientes es un protocolo que se utiliza entre el DTE Frame Relay y el switch Frame Relay?
   - **a.** VC
   - **b.** CIR
   - **c.** LMI
   - **d.** Q.921
   - **e.** DLCI
   - **f.** FRF.5
   - **g.** Encapsulación
2. ¿Cuáles de las afirmaciones siguientes son ciertas respecto a Frame Relay?
   - **a.** Normalmente, el DTE se encuentra en la ubicación del cliente.
   - **b.** Los routers envían mensajes LMI entre sí para indicar el estado de un VC.
   - **c.** El DLCI de origen de una trama tiene que permanecer intacto, pero el DLCI de destino de la trama se puede cambiar a medida que la trama recorre la nube de Frame Relay.
   - **d.** El tipo de encapsulación de Frame Relay que se aplica en el router remitente tiene que coincidir con el tipo de encapsulación del router de destino para que el router de destino pueda comprender el contenido de la trama.
3. ¿Qué significa DLCI?
   - **a.** Identificador de conexión de enlace de datos.
   - **b.** Indicador de conexión de enlace de datos.
   - **c.** Identificador de circuito de enlace de datos.
   - **d.** Indicador de circuito de enlace de datos.

4. El router R1 recibe una trama procedente del router R2, cuyo valor de DLCI es 222. ¿Cuál de las siguientes afirmaciones respecto a esta red es la más precisa?
   a. 222 representa al Router R1.
   b. 222 representa al Router R2.
   c. 222 es el DLCI de R1 que representa el VC existente entre R1 y R2.
   d. 222 es el DLCI local de R2 que representa el VC que existe entre R1 y R2.
5. Un diagrama de planificación de Frame Relay muestra el número 101 junto a R1, 102 junto a R2, 103 junto a R3, y 104 junto a R4. No se muestra ningún otro DLCI. El ingeniero jefe nos indica que el diagrama de planificación utiliza direccionamiento global de DLCI y que existe una malla completa de VCs. ¿Cuáles de las afirmaciones siguientes son verdaderas?
   a. Las tramas enviadas por R1 a R2, cuando atraviesan el enlace de acceso de R2, tienen el DLCI 102.
   b. Las tramas enviadas por R1 a R2, cuando atraviesan el enlace de acceso de R2, tienen el DLCI 101.
   c. Las tramas enviadas por R3 a R2, cuando atraviesan el enlace de acceso de R3, tienen el DLCI 102.
   d. Las tramas enviadas por R3 a R1, cuando atraviesan el enlace de acceso de R3, tienen el DLCI 102.
6. FredsCo tiene cinco sedes, cuyos routers están conectados a la misma red Frame Relay. Se han definido circuitos virtuales (VC) entre todas las parejas de routers. ¿Cuál es el menor número de subredes que podría utilizar FredsCo en la red Frame Relay?
   a. 1
   b. 2
   c. 3
   d. 4
   e. 5
   f. 10
7. BarneyCo tiene cinco sedes, cuyos routers están conectados a la misma red de Frame Relay. Se han definido VCs entre todas las parejas de routers. Barney, el director general de la compañía, está dispuesto a despedir a cualquier persona que configure Frame Relay sin utilizar subinterfaces punto a punto. ¿Cuál es el menor número de subredes que podría utilizar BarneyCo en la red Frame Relay?
   a. 1
   b. 4
   c. 8
   d. 10
   e. 12
   f. 15

8. R1 envía una trama de Frame Relay al router R2 a través de un VC. En ese mismo momento, un switch Frame Relay observa que hay demasiados paquetes que intentan abandonar la red Frame Relay a través del enlace de acceso que está conectado a R2. ¿Cuál de los siguientes es el resultado que tiene más probabilidades de ser producido por esta situación?

a. R1 acaba por recibir una trama que tiene activada la BECN.

b. R1 acaba por recibir una trama que tiene activada la FECN.

c. R1 acaba por recibir una trama que tiene activado DE.

d. Ninguna de las respuestas anteriores es correcta.

Temas fundamentales

Cuando se utilizan enlaces serie punto a punto, las compañías solicitan una línea alquilada, o circuito, que une dos puntos. La compañía de telecomunicaciones (telco) crea el circuito, e instala un cable de dos pares (con cuatro hilos) que llega a los edificios que se encuentran en ambos extremos del circuito. El proveedor crea el circuito de tal modo que funcione a la velocidad establecida y solicitada por el cliente, y que típicamente va a ser algún múltiplo de 64 kbps. En cuanto se ha conectado el cable de la telco a una CSU/DSU, y a un router en cada extremo del circuito, los routers disponen de un enlace físico dedicado, con la capacidad de enviar datos en ambas direcciones simultáneamente.

Frame Relay es un conjunto de estándares que crean un servicio WAN más eficiente que los enlaces punto a punto, aunque sigue permitiendo que las parejas de routers se envíen datos directamente entre sí. Cuando se utilizan líneas alquiladas, cada línea requiere una interfaz serie en cada router y un circuito físico exclusivo (y costoso) que construye la compañía de telecomunicaciones. Frame Relay tiene la capacidad de enviar datos a múltiples routers remotos a través de un único circuito WAN físico. Por ejemplo, una compañía que tenga una sede central y diez sedes remotas necesitaría diez líneas alquiladas para comunicarse con la sede central y diez interfaces serie en el router de la sede central. Si se utiliza Frame Relay, la sede central podría tener una sola línea alquilada que la conectase al servicio de Frame Relay y una sola interfaz serie en el router de la sede central, y seguiría pudiendo comunicarse con los diez routers de las sedes remotas.

La primera sección de este capítulo se centra en los fundamentos de Frame Relay, incluyendo mucha terminología. La segunda sección examina el direccionamiento de enlace de datos de Frame Relay. Este tema requiere una cierta atención, porque se necesitan direcciones de Frame Relay tanto para la configuración del router como para la resolución de problemas. Las dos últimas secciones principales de este capítulo examinan ciertos problemas de la capa de red que surgen al usar Frame Relay, junto con unas cuantas características que influyen sobre la velocidad y sobre las tasas de rechazo de tramas dentro de la nube de Frame Relay.

Visión general de Frame Relay

Las redes Frame Relay ofrecen más posibilidades y beneficios que los simples enlaces WAN punto apunto, pero para hacer esto los protocolos de Frame Relay son más minuciosos. Por ejemplo, las redes Frame Relay son redes multiacceso, lo cual significa que se pueden conectar a la red más de dos dispositivos, de forma similar a las LANs. A diferencia de las LANs, no es posible enviar una difusión de capa de enlace de datos a través de Frame Relay. Por tanto, las redes Frame Relay se denominan redes **multiacceso sin difusión** (*nonbroadcast multiaccess*, NBMA). Además, como Frame Relay es multiacceso, exige utilizar una dirección que identifique a qué router remoto está dirigida cada trama.

La Figura 13.1 muestra la topología física básica, y la terminología relacionada con las redes Frame Relay.

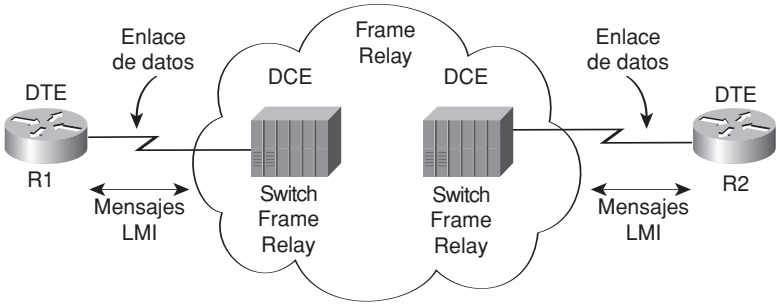


Figura 13.1. Componentes de Frame Relay.

La Figura 13.1 muestra los componentes más básicos de una red Frame Relay. Se instala una línea alquilada entre el router y un switch Frame Relay cercano; este enlace se denomina **enlace de acceso**. Para asegurar que el enlace está funcionando, el dispositivo situado fuera de la red Frame Relay, que se denomina **equipo terminal de datos** (*data terminal equipment*, *DTE*), intercambia mensajes regularmente con el switch Frame Relay. Estos mensajes *keepalive*, junto con otros mensajes, están definidos por el protocolo de Frame Relay **Interfaz de administración local** (*Local Management Interface*, *LMI*). Los routers se consideran DTE, y los switches Frame Relay reciben el nombre de **equipo de comunicación de datos** (*data communications equipment*, *DCE*).

La Figura 13.1 muestra la conectividad física de cada conexión a la red Frame Relay, mientras que la Figura 13.2 muestra la conectividad lógica punto a punto, o conectividad virtual, que está asociada a un circuito virtual (VC).

La ruta lógica de comunicaciones entre cada pareja de DTEs es un VC. El trío de líneas paralelas que hay en la figura representa un único VC; este libro emplea trazos gruesos discontinuos para garantizar que se vea bien la línea. Típicamente, el proveedor de servicios preconfigura todos los detalles del VC; los VCs predefinidos se denominan circuitos virtuales permanentes (PVC).

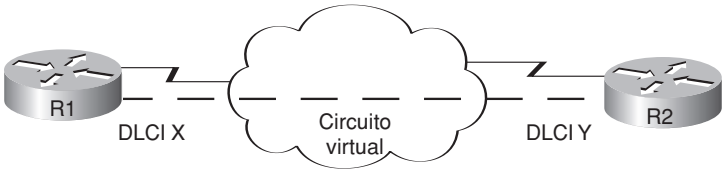


Figura 13.2. Conceptos de PVC Frame Relay.

Los routers utilizan el identificador de conexión de enlace de datos (DLCI) como dirección de Frame Relay; esto identifica el VC a través del que debe viajar la trama. Por tanto, en la Figura 13.2, cuando R1 necesita enviar un paquete a R2, R1 encapsula el paquete de capa 3 en una cabecera y una información final Frame Relay y después envía la trama. El encabezado de Frame Relay contiene el DLCI correcto, de tal modo que los switches Frame Relay del proveedor puedan reenviar correctamente la trama a R2.

La Tabla 13.2 muestra los componentes que aparecen en las Figuras 13.1 y 13.2, junto con algunos términos asociados. Después de la tabla se describen con más detalle las características más importantes de Frame Relay.

Tabla 13.2. Términos y conceptos de Frame Relay.

Términos	Descripción
Circuito virtual (VC)	Es un concepto lógico que representa la ruta que recorren las tramas entre dos DTEs. Los VCs son especialmente útiles cuando se compara Frame Relay con los circuitos físicos alquilados.
Circuito virtual permanente (PVC)	VC predefinido. Conceptualmente, se puede considerar que un PVC equivale a una línea alquilada.
Circuito virtual conmutado (SVC)	Un VC que se configura dinámicamente cuando es necesario. Conceptualmente, se puede considerar que un SVC es equivalente a una conexión por vía telefónica.
Equipo terminal de datos (DTE)	Los DTEs se conectan a un servicio Frame Relay de una compañía de telecomunicaciones. Típicamente, residen en las sedes que utiliza la compañía que adquiere el servicio Frame Relay.
Equipo de comunicación de datos (DCE)	Los switches Frame Relay son dispositivos DCE. Los DCEs también se conocen con el nombre de equipos de terminación de circuito. Típicamente, los DCEs se encuentran en la red del proveedor de servicios.
Enlace de acceso	Es la línea alquilada que media entre el DTE y el DCE.
Velocidad de acceso (AR)	Velocidad de reloj del enlace de acceso. Esta opción afecta al precio de la conexión.

(continúa)

Tabla 13.2. Términos y conceptos de Frame Relay *(continuación)*.

Término	Descripción
Velocidad de información suscrita (CIR)	Velocidad con que se pueden enviar bits a través de un VC, de acuerdo con el contrato comercial existente entre el cliente y el proveedor.
Identificador de conexión de enlace de datos (DLCI)	Dirección de Frame Relay que se utiliza en los encabezados de Frame Relay para identificar el VC.
Multiacceso sin difusión (NBMA)	Una red en la cual no se admiten las difusiones, pero se pueden conectar más de dos dispositivos.
Interfaz de administración local (LMI)	Protocolo que se utiliza entre un DCE y un DTE para administrar la conexión. Los mensajes de señalización para SVC, los mensajes de estado de PVC y los *keepalives* son todos mensajes LMI.

Estándares de Frame Relay

Las definiciones de Frame Relay se encuentran en documentos de la International Telecommunications Union (ITU, Unión internacional de las telecomunicaciones) y del American National Standards Institute (ANSI, Instituto nacional americano de normalización). El Frame Relay Forum (http://www.frforum.com), que es un consorcio de fabricantes, define también varias especificaciones de Frame Relay, muchas de las cuales anteceden a las especificaciones originales de la ITU y del ANSI; tanto ITU como ANSI han adoptado muchos de los estándares del foro. La Tabla 13.3 muestra las más importantes de estas especificaciones.

Tabla 13.3. Especificaciones del protocolo Frame Relay.

Qué define la especificación	Documento ITU	Documento ANSI
Especificaciones de enlace de datos, incluyendo encabezado e información de LAPF	Q.922 Anexo A (Q.922-A)	T1.618
Administración de PVC, LMI	Q.933 Anexo A (Q.933-A)	T1.617 Anexo D (T1.617-D)
Señalización SVC	Q.933	T1.617
Encapsulamiento multiprotocolo (basado en la RFC 1490/2427)	Q.933 Anexo E (Q.933-E)	T1.617 Anexo F (T1.617-F)

Circuitos Virtuales

Frame Relay ofrece ventajas significativas respecto a utilizar simplemente líneas alquiladas punto a punto. La ventaja principal está relacionada con los circuitos virtuales. Considere la Figura 13.3, que muestra una red Frame Relay típica con tres sedes.

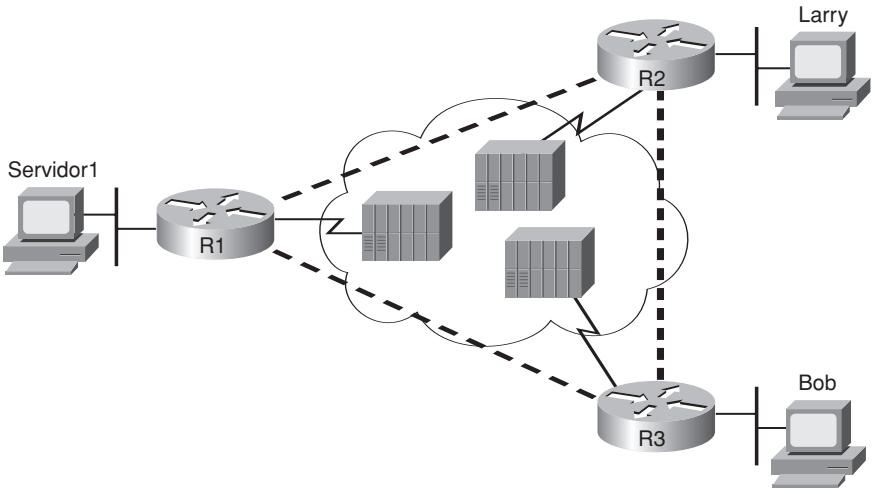


Figura 13.3. Red Frame Relay típica con tres sedes.

Los circuitos virtuales definen una ruta lógica entre dos DTEs de Frame Relay. El término **circuito virtual** describe bien el concepto. Se comporta como un circuito punto a punto, y ofrece la posibilidad de enviar datos entre dos puntos finales a través de una WAN. No existe un circuito físico directo entre los dos puntos finales, así que es un circuito virtual. Por ejemplo, R1 es el final de dos VCs; uno cuyo otro extremo es R2 y otro cuyo otro extremo es R3. R1 puede enviar tráfico directamente a cualquiera de los otros dos routers, enviándolo a través del VC oportuno.

Los VCs comparten el enlace de acceso y la red Frame Relay. Por ejemplo, los dos VCs que terminan en R1 comparten un mismo enlace de acceso. De hecho, muchos clientes comparten la misma red Frame Relay. Originalmente, las personas que tenían redes basadas en líneas alquiladas sentían cierta reticencia a pasar a Frame Relay, porque sería preciso compartir la capacidad ofrecida por el proveedor con los demás clientes dentro de la nube. Para descartar este problema, Frame Relay se ha diseñado con el concepto de una velocidad de información suscrita (CIR). Cada VC posee una CIR, que es la garantía ofrecida por el proveedor de que un cierto VC va a disponer al menos de ese ancho de banda. Por tanto, se puede migrar de una línea alquilada a Frame Relay, obteniendo una CIR de al menos tanto ancho de banda como se tuviera anteriormente con una línea alquilada.

Curiosamente, aunque se tenga una red que llegue a tres sedes, es probable que resulte menos costoso utilizar Frame Relay que enlaces punto a punto. Considere una organización con 100 sedes que necesite conectividad en todas partes. ¿Cuántas líneas alquiladas se necesitan? ¡4950! Y además, la organización necesitaría 99 interfaces serie por router si utilizase líneas alquiladas punto a punto. Si se utiliza Frame Relay, la organización puede tener 100 enlaces de acceso a switches Frame Relay locales, uno por router, y usar 4950 VCs funcionando a través de ellos. Esto requiere un número mucho menor de enlaces físicos reales, ¡y sólo se necesitaría una interfaz serie en cada router!

Los proveedores de servicios pueden construir redes Frame Relay con menos costes que si se utilizaran líneas alquiladas. Como cabría esperar, esto hace que Frame Relay resulte menos costoso también para el cliente. Para conectarse a múltiples sitios de una WAN, Frame Relay es más eficiente en términos de coste que las líneas alquiladas.

Se admiten dos tipos de VCs: los permanentes (PVC) y los conmutados (SVC). Los PVCs están predefinidos por el proveedor; los SVCs se crean dinámicamente. Los PVCs son, con mucho, los más populares de los dos. Los proveedores de Frame Relay rara vez ofrecen los SVCs como servicio. (El resto de este capítulo y el Capítulo 14 ignoran los SVCs.)

Cuando se configure una red Frame Relay, es posible que el diseño no incluya un VC entre cada pareja de sedes. La Figura 13.3 posee un PVC entre cada pareja de sedes; esto se llama una red Frame Relay de malla completa. Cuando no todas las parejas tienen un PVC directo, se habla de una red de malla parcial. La Figura 13.4 muestra la misma red que la Figura 13.3, pero esta vez con una malla parcial y solo dos PVCs. Esto es típico cuando R1 se encuentra en la sede principal y R2 y R3 son oficinas remotas que raramente necesitan comunicarse directamente.

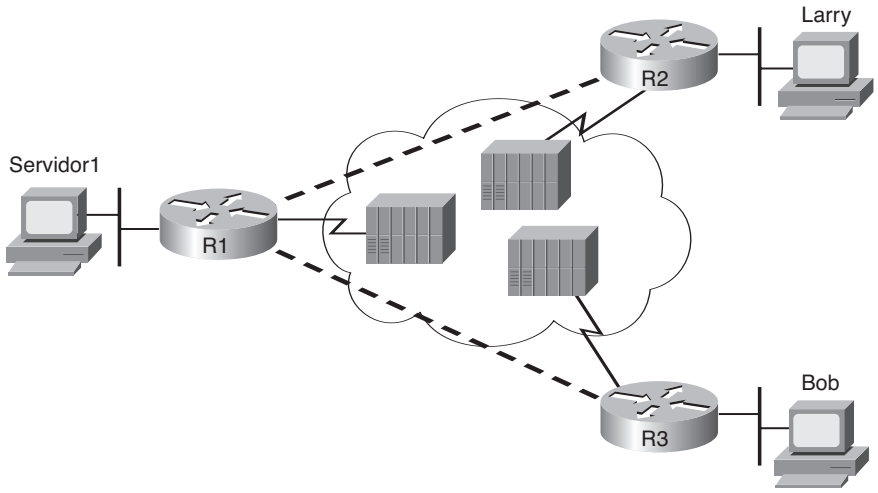


Figura 13.4. Red Frame Relay típica de malla parcial.

La malla parcial posee ciertas ventajas y desventajas en comparación con una malla completa. La ventaja principal es que la malla parcial es más barata porque el proveedor tarifica por cada VC. La desventaja es que el tráfico que vaya desde R2 hasta R3 debe ir primero a R1 para ser reenviado. Si es una pequeña cantidad de tráfico, no tiene importancia. Si es mucho tráfico, es probable que merezca la pena el coste adicional de una malla completa, porque el tráfico que circula entre dos sitios remotos va a tener que cruzar dos veces el enlace de acceso de R1.

Una dificultad conceptual de los PVCs es que típicamente hay un único enlace de acceso a través del cual pasan múltiples PVCs. Por ejemplo, considere la Figura 13.4 desde el

punto de vista de R1. El Servidor1 envía un paquete a Larry. Llega a través de Ethernet. R1 lo compara con la tabla de enrutamiento de Larry, que le indica que envíe el paquete a través de Serial0, que es el enlace de acceso de R1. El router encapsula el paquete en un encabezado e información final de Frame Relay y lo envía. ¿Qué PVC debe usar? El switch Frame Relay debería enviárselo a R2, pero ¿por qué?

Para resolver este problema, Frame Relay hace uso de una dirección para distinguir un PVC de otro. Esta dirección se llama Identificador de conexión de enlace de datos (DLCI). El nombre es descriptivo: la dirección corresponde a un protocolo ISO de la capa 2 (un enlace de datos), e identifica a un VC, que a veces se denomina **conexión virtual**. Por tanto, en este ejemplo, R1 utiliza el DLCI que identifica el PVC asociado a R2, así que el proveedor reenvía correctamente la trama a través del PVC hasta R2. Para enviar tramas a R3, R1 utiliza el DLCI que identifica el VC de R3. Los DLCIs y la forma en que funcionan se tratan con más detalle más adelante en este capítulo.

LMI y tipos de encapsulación

Cuando se empieza a aprender acerca de Frame Relay, es fácil confundir la LMI y la encapsulación que se utiliza con Frame Relay. La LMI es una definición de los mensajes que se emplean entre el DTE (por ejemplo, un router) y el DCE (por ejemplo, el switch Frame Relay cuyo dueño es el proveedor de servicios). La encapsulación define los encabezados que utiliza el DTE para comunicar información al DTE que se encuentra al otro extremo del VC. El switch y el router al que está conectado se encargan de utilizar la misma LMI; el switch no se preocupa de la encapsulación. Los routers de los extremos (los DTEs) sí se ven afectados por la encapsulación.

El mensaje LMI más importante en relación con los temas del examen es el mensaje de consulta de estado LMI. Los mensajes de estado tienen dos misiones clave:

- Tienen una función de recordatorio entre el DTE y el DCE. Si el enlace de acceso tiene un problema, la ausencia de mensajes *keepalive* implica que el enlace ha fallado.
- Indican si un PVC está activo o inactivo. Aunque los PVCs están predefinidos, su estado puede cambiar. Un enlace de acceso podría estar activado, pero uno o más VCs podrían estar desactivados. El router necesita saber qué VCs están activos y cuáles están inactivos. Esta información la obtiene del switch, empleando mensajes de estado de LMI.

En el software IOS de Cisco están disponibles tres opciones de protocolo LMI: Cisco, ITU y ANSI. Cada opción de LMI es ligeramente diferente y, por tanto, incompatible con las otras dos. Siempre y cuando el DTE y el DCE de cada extremo de un enlace de acceso utilicen el mismo estándar de LMI, LMI funcionará perfectamente.

Las diferencias entre tipos de LMI son sutiles. Por ejemplo, la LMI de Cisco requiere utilizar el DLCI 1023, mientras que ANSI T1.617-D e ITU Q.933-A especifican el DLCI 0. Algunos de los mensajes tienen campos distintos en sus encabezados. El DTE necesita simplemente saber cuál de los tres LMIs debe utilizar para que pueda usar el mismo que el switch local.

Es fácil configurar el tipo de LMI. La opción más popular en la actualidad consiste en emplear la configuración predeterminada de LMI. Esta configuración emplea la característica de autodetección de LMI, consistente en que el router se limita a averiguar qué tipo de LMI está empleando el switch. Por tanto, podemos limitarnos a hacer que el router autodetecte la LMI, sin molestarnos en codificar el tipo de LMI. Si se opta por configurar el tipo de LMI, el router desactiva la característica de autodetección.

La Tabla 13.4 muestra los tres tipos de LMI, su origen y la palabra reservada que se utiliza en el subcomando de interfaz frame-relay lmi-type que ofrece el software IOS de Cisco.

Tabla 13.4. Tipos de LMI en Frame Relay

Nombre	Documento	Parámetro de tipo de LMI en el IOS
Cisco	Propio	cisco
ANSI	T1.617 Anexo D	ansi
ITU	Q.933 Anexo A	q933a

Los routers conectados mediante Frame Relay encapsulan los paquetes de capa 3 en un encabezado y una información final de Frame Relay antes de enviarlos a través del enlace de acceso. El encabezado y la información final están definidos por la especificación de Servicios de transporte de tramas para el Procedimiento de acceso a través de un enlace (*Link Access Procedure Frame Bearer Services*, LAPF), ITU Q.922-A. El tramado LAPF disperso ofrece detección de errores mediante una FCS que va en la información final, y también los campos DLCI, DE, FECN y BECN en el encabezado (que se describen posteriormente). La Figura 13.5 es una representación de la trama.

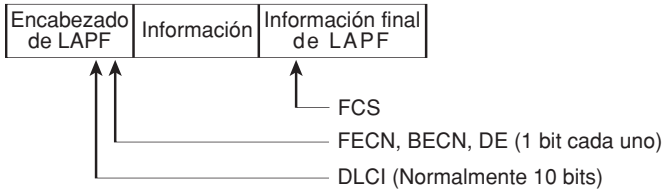


Figura 13.5. Encabezado LAPF.

Sin embargo, el encabezado y la información final de LAPF no ofrecen todos los campos que necesitan típicamente los routers. En particular, la Figura 13.5 no muestra un campo de Tipo de protocolo. Todo encabezado de enlace de datos requiere un campo que defina el tipo de paquete que sigue al encabezado de enlace de datos. Si Frame Relay sólo está empleando el encabezado LAPF, los DTEs (incluyendo los routers) no pueden admitir tráfico multiprotocolo, porque no hay manera de identificar el tipo de protocolo en el campo Información.

Para compensar la falta de un campo de Tipo de protocolo en el encabezado estándar de Frame Relay se han ideado dos soluciones:

- Cisco y otras tres compañías crearon un encabezado adicional, que se intercala entre el encabezado LAPF y el paquete de la Capa 3 que se muestra en la Figura 13.5. Incluye un campo de Tipo de protocolo de 2 bytes, con valores que coinciden con los de ese mismo campo, que Cisco utiliza para HDLC.
- La RFC 1490 (que fue reemplazada posteriormente por la RFC 2427; hay que conocer los dos números), *Multiprotocol Interconnect over Frame Relay* (interconexión multiprotocolo a través de Frame Relay), definió la segunda solución. La RFC1490 se escribió para asegurar la interoperabilidad entre fabricantes de DTE para Frame Relay. Esta RFC define un encabezado similar, que también se ubica entre el encabezado LAPF y el paquete de capa 3, e incluye un campo de Tipo de protocolo así como muchas otras opciones. Posteriormente, ITU y ANSI unieron los encabezados de la RFC 1490 a sus especificaciones Q.933 Anexo E y T1.617 Anexo F.

La Figura 13.6 muestra estas dos alternativas.

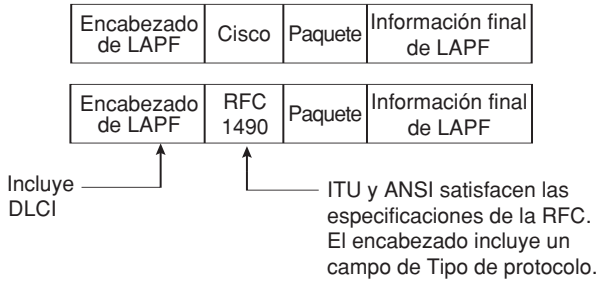


Figura 13.6. Encapsulación de Cisco y de la RFC 1490/2427.

Los DTEs utilizan y reconocen los campos especificados por estos dos tipos de encapsulación, pero los switches Frame Relay ignoran estos campos. *Como las tramas van de DTE a DTE, ambos DTEs tienen que estar de acuerdo respecto a la encapsulación utilizada. A los switches les da igual.* Sin embargo, cada VC puede utilizar una encapsulación diferente. En la configuración, la encapsulación creada por Cisco se denomina `cisco`, y la otra se denomina `ietf`.

Ahora que ya disponemos de una comprensión general de los conceptos y la terminología de Frame Relay, la sección siguiente examina con mucho más detalle los DLCIs de Frame Relay.

Direccionamiento en Frame Relay

Frame Relay define las reglas mediante las cuales los dispositivos entregan tramas Frame Relay a través de las redes Frame Relay. Como el router emplea un único enlace de

acceso que posee muchos VCs que lo conectan a muchos routers, tiene que existir algo que identifique a cada uno de los routers remotos; en otras palabras, una dirección. El DLCI es la dirección de Frame Relay.

Los DLCIs operan de forma ligeramente distinta de las otras direcciones de enlace de datos que se tratan en los exámenes de CCNA. Esta diferencia se debe especialmente al uso del DLCI y al hecho consistente en que *el encabezado posee un único campo DLCI, y no dos campos DLCI de origen y de destino.*

Direccionamiento local en Frame Relay

Es preciso entender unas cuantas características de los DLCIs antes de enfrentarnos a su utilización. Los DLCIs son significativos localmente; esto significa que las direcciones sólo necesitan ser exclusivas en el enlace de acceso local. Una analogía popular que explica el direccionamiento local consiste en que sólo puede haber una dirección de la forma 2000 Pennsylvania Avenue en Washington, DC, pero puede existir la dirección 2000 Pennsylvania Avenue en cualquier ciudad de los Estados Unidos de América. De forma similar, los DLCIs tienen que ser exclusivos en cada enlace de acceso, pero se pueden emplear los mismos números de DLCI en todos los enlaces de acceso de nuestra red. Por ejemplo, en la Figura 13.7, obsérvese que se utiliza el DLCI 40 en dos enlaces de acceso para describir dos PVCs distintos. No hay conflicto, porque el DLCI 40 se utiliza en dos enlaces de acceso diferentes.

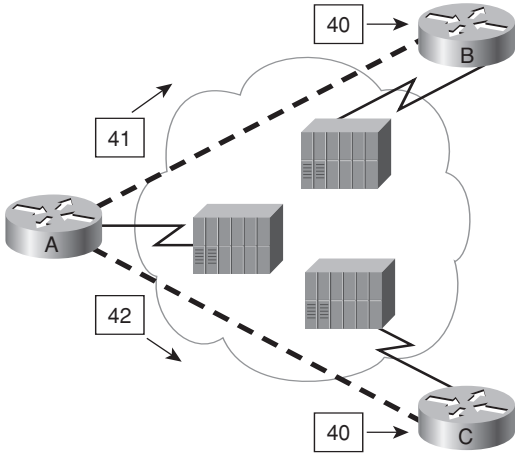


Figura 13.7. Direccionamiento de Frame Relay en el que el Router A envía información a los Routers B y C.

El direccionamiento local, que es el término común para indicar que los DLCIs son significativos localmente, es un hecho. Esa es la forma en que opera Frame Relay. Dicho simplemente, un solo enlace de acceso no puede utilizar el mismo DLCI para representar

múltiples VCs en el mismo enlace de acceso. Si no fuera así, el switch Frame Relay no sería capaz de reenviar correctamente las tramas. Por ejemplo, en la Figura 13.7, el Router A se ve obligado a utilizar valores distintos de DLCI para los PVCs de su enlace de acceso local (41 y 42 en este caso).

Direccionamiento global en Frame Relay

Muchas personas se sienten confusas respecto a los DLCIs cuando piensan por primera vez acerca del significado local de los DLCIs, y observan que existe un único campo DLCI en el encabezado de Frame Relay. El direccionamiento global resuelve este problema, haciendo que el direccionamiento DLCI parezca un direccionamiento LAN conceptualmente. El direccionamiento global es simplemente una forma de seleccionar números de DLCI cuando se planifica una red Frame Relay de tal modo que resulta mucho más sencillo trabajar con DLCIs. Como el direccionamiento local es un hecho, el direccionamiento global no cambia estas reglas. El direccionamiento global sólo hace que la asignación de DLCI sea más evidente… en cuanto uno se acostumbra.

Veamos la forma en que funciona el direccionamiento global: el proveedor de servicios entrega una hoja de cálculo con la planificación, y un diagrama. La Figura 13.8 es un ejemplo de uno de estos diagramas, y se muestran los DLCIs globales.

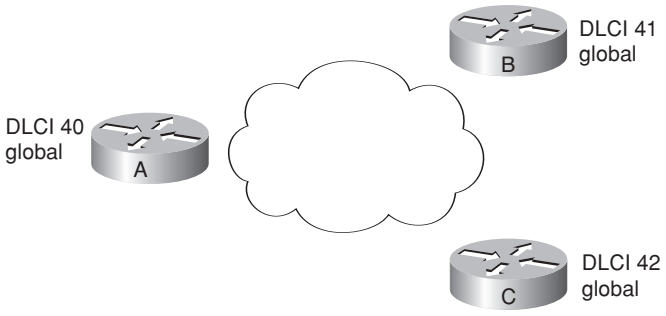


Figura 13.8. DLCIs globales de Frame Relay.

El direccionamiento global se planifica tal como se muestra en la Figura 13.8, con los DLCIs que se pondrán en las tramas de Frame Relay según puede verse en la Figura 13.9. Por ejemplo, el Router A emplea el DLCI de valor 41 cuando envía tramas al Router B, porque el DLCI global del Router B es 41. De forma similar, el Router A utiliza el DLCI 42 cuando envía tramas a través del VC con destino al Router C. Lo mejor es que el direccionamiento global es mucho más lógico para casi todas las personas, porque se comporta como una LAN, con una sola dirección MAC para cada dispositivo. En una LAN, si las direcciones MAC son MAC-A, MAC-B y MAC-C para los tres routers, entonces el Router A utiliza la dirección de destino MAC-B cuando envía tramas al Router B, y utiliza la

MAC-C como destino para llegar al Router C. De forma similar, cuando se utilizan los DLCIs globales 40, 41 y 42 para los Routers A, B y C respectivamente, se aplica el mismo concepto. Como los DLCIs aluden a VC, la lógica cuando el Router A envía tramas al Router B es similar a esta: "¡Atención, switch local! Cuando recibas esta trama, envíala a través del VC que hemos acordado numerar con el DLCI 41". La Figura 13.9 muestra este ejemplo.

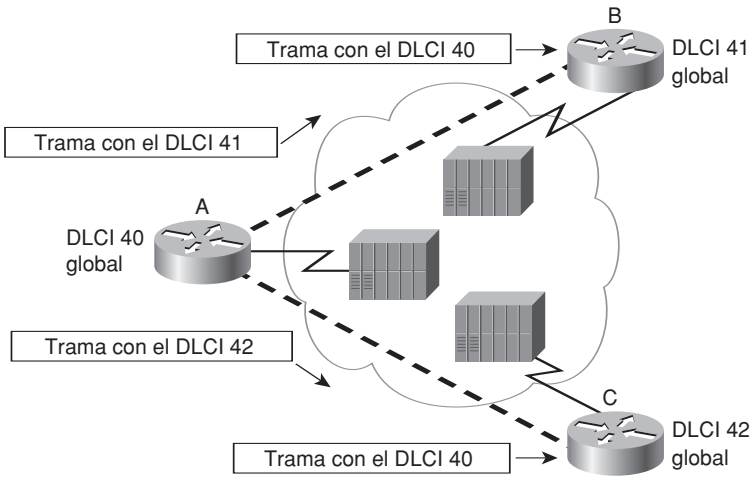


Figura 13.9. Direccionamiento global de Frame Relay desde el punto de vista del remitente.

El Router A envía tramas cuyo DLCI es 41, y estas llegan al switch local. El switch local observa el campo DLCI y reenvía la trama por la red Frame Relay hasta que ésta llega al switch conectado al Router B. El mismo proceso se produce entre el Router B y el C cuando el Router A utiliza el DLCI 42. Lo interesante del direccionamiento global es que uno piensa que cada router tiene una dirección, como en el direccionamiento de una LAN. Si se desea enviar una trama a algún sitio, se pone su DLCI en el encabezado, y la red entrega la trama al DTE correcto.

La clave final del direccionamiento global es que los switches Frame Relay cambian verdaderamente el valor del DLCI antes de entregar la trama. ¿Ha observado que en la Figura 13.9 se muestra un valor distinto de DLCI cuando las tramas son recibidas por los Routers B y C? Por ejemplo, el Router A envía una trama al Router B, y el Router B pone en la trama el DLCI 41. El último switch asigna al campo de DLCI el valor 40 antes de reenviarlo al Router B. El resultado es que cuando los Routers B y C reciben sus tramas, el valor de DLCI es realmente el DLCI del emisor. ¿Por qué? Cuando el Router B recibe la trama, como el DLCI es 40, sabe que la trama ha entrado a través del PVC que hay entre sí mismo y el Router A. En general, ocurre lo siguiente:

- El emisor trata el campo de DLCI como dirección de destino, y emplea el DLCI global del destinatario en el encabezado.

- El receptor considera que el campo DLCI es la dirección del remitente, porque contiene el DLCI global de quien ha enviado la trama.

La Figura 13.9 describe lo que sucede en una red Frame Relay típica. Los proveedores de servicios proporcionan una hoja de cálculo con la planificación y unos diagramas en que se muestran los DLCIs globales. La Tabla 13.5 ofrece una visión organizada de los DLCIs que se utilizan en la Figura 13.9.

Tabla 13.5. Intercambio de DLCI en la nube Frame Relay de la Figura 13.9.

La trama enviada por el router	cuyo campo DLCI contiene	se entrega al router	con este valor en el campo DLCI
A	41	B	40
A	42	C	40
B	40	A	41
C	40	A	42

El direccionamiento global hace que el direccionamiento DLCI resulte más intuitivo para la mayoría de las personas. También hace más sencilla la configuración de routers y permite añadir sitios nuevos con más comodidad. Por ejemplo, considere la Figura 13.10, que añade a la red los Routers D y E. El proveedor de servicios se limita a indicar que los DLCIs globales 43 y 44 se emplean para esos dos routers. Si esos dos routers también disponen de un único PVC hacia el Router A, toda la planificación de DLCI está completa. Se sabe que los Routers D y E emplean el DLCI 40 para llegar al Router A, y que el Router A utiliza el DLCI 43 para llegar al Router D y el DLCI 44 para llegar al Router E.

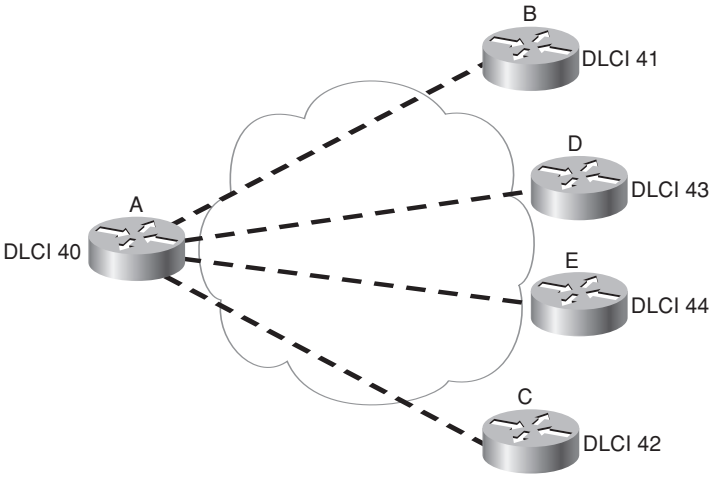


Figura 13.10. Adición de sedes en Frame Relay: direccionamiento global.

Los ejemplos restantes de este capítulo utilizan el direccionamiento global en todos los diagramas de planificación, salvo indicación expresa en contra. Una forma práctica de determinar si el diagrama muestra los DLCI locales o los globales es la siguiente: si dos VCs terminan en el mismo DTE y se muestra un solo DLCI, es probable que represente la convención de DLCI global. Si se muestra un DLCI por VC, se está representando un direccionamiento DLCI local.

Ahora que ya comprendemos mejor la forma en que Frame Relay utiliza los DLCIs para acceder a cada VC, dando lugar a la correcta entrega de tramas a través de una nube Frame Relay, la sección siguiente pasa a la capa 3, y examina las convenciones de direccionamiento IP que se pueden utilizar a través de Frame Relay.

Temas de la capa de red relativos a Frame Relay

Las redes Frame Relay tienen tanto analogías como diferencias con respecto a los enlaces WAN punto a punto. Estas diferencias introducen algunas consideraciones adicionales cuando se pasan paquetes de la capa 3 a través de una red Frame Relay. Hay que ocuparse de un par de cuestiones importantes respecto a los flujos de la capa 3 a través de Frame Relay:

- La selección de direcciones de la capa 3 en interfaces Frame Relay.
- La manipulación de la difusión.

En particular, la implementación de Frame Relay que ofrece Cisco define tres opciones diferentes para asignar subredes y direcciones IP en las interfaces Frame Relay:

- Una subred que contiene todos los DTEs de Frame Relay.
- Una subred por VC.
- Un híbrido de las dos primeras opciones.

Esta sección examina las tres opciones principales de direccionamiento IP a través de Frame Relay, así como la manipulación de la difusión, que influye en la forma en que funcionan los protocolos de enrutamiento a través de Frame Relay.

Direccionamiento de capa 3 en Frame Relay: una subred que contiene todos los DTEs de Frame Relay

La Figura 13.11 muestra la primera alternativa, que consiste en utilizar una sola subred para la red Frame Relay. La figura muestra una red Frame Relay de malla completa porque la opción de una sola subred se utiliza típicamente cuando existe una malla completa de VCs. En una malla completa, cada router posee un VC que llega a todos los demás routers, lo cual significa que cada router puede enviar directamente tramas a cualquier otro router. Esto se

parece especialmente a la forma en que funciona una LAN. Por tanto, se puede utilizar una sola subred para todas las interfaces Frame Relay del router, como se configuran las interfaces serie del router. La Tabla 13.6 resume las direcciones que se utilizan en la Figura 13.11.

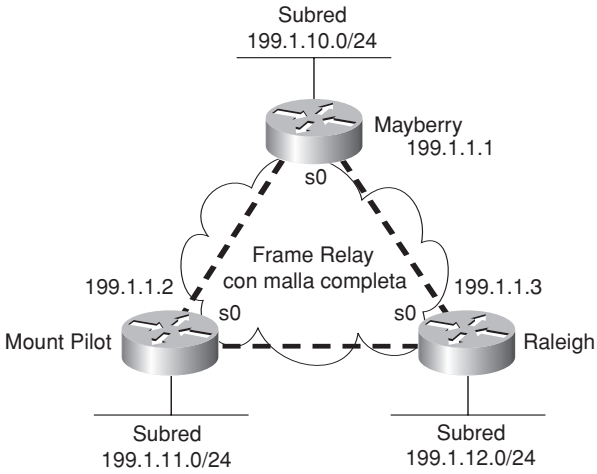


Figura 13.11. Malla completa con direcciones IP.

Tabla 13.6. Direcciones IP sin subinterfaces.

Router	Dirección IP de la interfaz Frame Relay
Mayberry	199.1.1.1
Mount Pilot	199.1.1.2
Raleigh	199.1.1.3

La alternativa de una sola subred es sencilla, y reduce la utilización del espacio de direcciones IP. Se parece a lo que uno está acostumbrado a ver en las LANs, lo cual hace que resulte más fácil de conceptualizar. Desafortunadamente, casi todas las compañías construyen redes Frame Relay de malla parcial, y la opción de subred única posee algunas deficiencias cuando la red es una malla parcial.

Direccionamiento de capa 3 en Frame Relay: una subred por VC

La segunda alternativa de direccionamiento IP, que consiste en tener una sola subred para cada VC, funciona mejor con una red Frame Relay de malla parcial, según se muestra

en la Figura 13.12. Boston no puede reenviar directamente tramas a Charlotte, porque no se ha definido un VC entre ambos. Se trata de una red Frame Relay más típica, porque la mayor parte de las organizaciones con muchas sedes tienden a agrupar las aplicaciones en servidores situados en unas pocas ubicaciones centralizadas, y la mayor parte del tráfico se produce entre las sedes remotas y esos servidores.

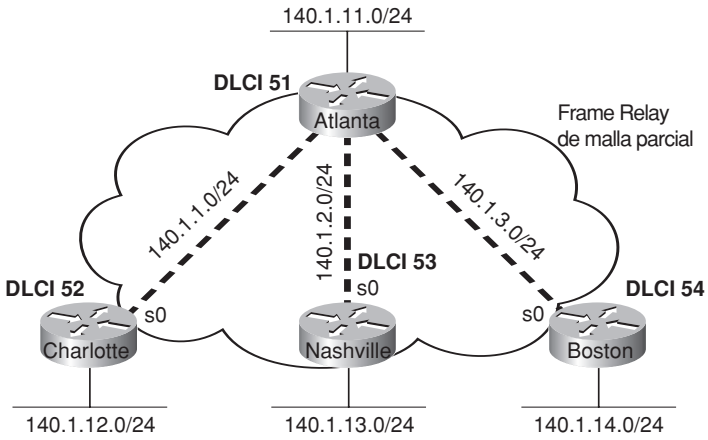


Figura 13.12. Malla parcial con direcciones IP.

La alternativa de una sola subred por VC sigue la lógica de un conjunto de enlaces punto a punto. Al utilizar múltiples subredes en lugar de una sola subred más extensa se desperdician algunas direcciones IP, pero se superan algunos problemas asociados a protocolos de enrutamiento por vector de distancia.

La Tabla 13.7 muestra las direcciones IP de una red Frame Relay de malla parcial que se muestra en la Figura 13.12.

Tabla 13.7. Direcciones IP con subinterfaces punto a punto.

Router	Subred	Dirección IP
Atlanta	140.1.1.0	140.1.1.1
Charlotte	140.1.1.0	140.1.1.2
Atlanta	140.1.2.0	140.1.2.1
Nashville	140.1.2.0	140.1.2.3
Atlanta	140.1.3.0	140.1.3.1
Boston	140.1.3.0	140.1.3.4

El software IOS de Cisco tiene una característica de configuración llamada **subinterfaces**, que crea una subdivisión lógica en una interfaz física. Las subinterfaces permiten que el router Atlanta tenga asociadas tres direcciones IP a su interfaz física Serial0, configurando tres subinterfaces separadas. El router puede acceder a todas las subinterfaces, y al VC asociado a cada una de ellas, como si se tratasen de enlaces serie punto a punto. Cada una de las tres subinterfaces de Serial0 de Atlanta tendría asignada una dirección IP distinta de las que constan en la Tabla 13.7 (el Capítulo 14 muestra varios ejemplos de configuración).

Nota

El ejemplo utiliza unos prefijos de dirección IP iguales a /24 para simplificar los cálculos. En las redes de producción, las subinterfaces punto a punto utilizan típicamente un prefijo de /30 (con la máscara 255.255.255.252), porque esto sólo permite dos direcciones IP válidas: es el número exacto que se necesita para una subinterfaz punto a punto. Por supuesto, utilizar distintas máscaras en una misma red significa que el protocolo de enrutamiento también debe admitir VLSM.

Direccionamiento de capa 3 en Frame Relay: método híbrido

La tercera alternativa para el direccionamiento de capa 3 es un híbrido de las dos primeras. Considere la Figura 13.13, que muestra un trío de routers con VCs entre todos ellos, así como otros dos VCs que van a sedes remotas.

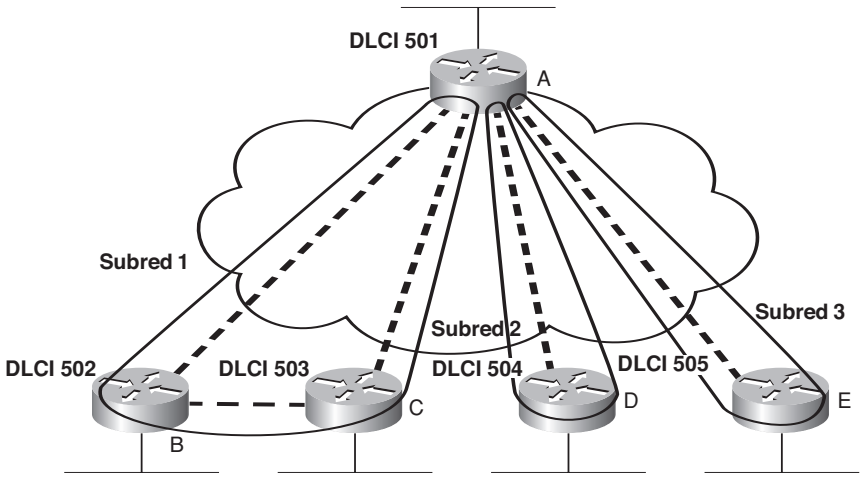


Figura 13.13. Híbrido de malla total y parcial.

En este caso existen dos opciones para el direccionamiento de capa 3. La primera consiste en tratar a cada VC como un grupo distinto de capa 3. En este caso, se necesitan cinco subredes para la red Frame Relay. Sin embargo, los Routers A, B y C crean una malla completa más pequeña entre sí. Esto permite a los Routers A, B y C utilizar una subred. Los otros dos VCs, uno entre los Routers A y D y otro entre los Routers A y E, se tratan como dos grupos distintos de capa 3. El resultado es un total de tres subredes.

Para obtener cualquiera de estos estilos de direccionamiento de la capa 3 en este tercer y último caso, se utilizan subinterfaces. Las subinterfaces punto a punto se emplean cuando se estima que lo único que hay en el grupo es un solo VC; por ejemplo, entre los Routers A y E. Se utilizan subinterfaces multipunto cuando se considera que más de dos routers están en el mismo grupo; por ejemplo, con los Routers A, B y C.

Las subinterfaces multipunto terminan lógicamente en más de un VC. De hecho, el nombre "multipunto" implica la función, porque se puede llegar a más de una sede remota a través de un VC asociado a una subinterfaz multipunto.

La Tabla 13.8 resume las direcciones y subinterfaces que se emplean en la Figura 13.13.

Tabla 13.8. Direcciones IP con subinterfaces punto a punto y multipunto.

Router	Subred	Dirección IP	Tipo de subinterfaz
A	140.1.1.0/24	140.1.1.1	Multipunto
B	140.1.1.0/24	140.1.1.2	Multipunto
C	140.1.1.0/24	140.1.1.3	Multipunto
A	140.1.2.0/24	140.1.2.1	Punto a punto
D	140.1.2.0/24	140.1.2.4	Punto a punto
A	140.1.3.0/24	140.1.3.1	Punto a punto
E	140.1.3.0/24	140.1.3.5	Punto a punto

¿Qué es lo que se verá en una red real? La mayor parte del tiempo se utilizan interfaces punto a punto, con una sola subred por PVC. Sin embargo, uno debe comprender todas las opciones para los exámenes de CCNA.

Nota

El Capítulo 14 ofrece configuraciones completas para los tres casos que se ilustran en las Figuras 13.11, 13.12 y 13.13.

Manipulación de la difusión de capa 3

Después de enfrentarnos al direccionamiento de capa 3 a través de Frame Relay, hay que pasar a considerar la forma de tratar las difusiones a través de la capa 3. Frame Relay puede enviar copias de una difusión a través de todos los VCs, pero no existe un equivalente de las difusiones de una LAN. En otras palabras, no existe la posibilidad de que un DTE de Frame Relay envíe una sola trama a la red Frame Relay, dando lugar a que esa trama sea duplicada y entregada en múltiples destinos a través de múltiples VCs. Sin embargo, los routers necesitan efectuar difusiones para que funcionen varias características. En particular, las actualizaciones de protocolos de enrutamiento son difusiones o multidifusiones.

La solución del dilema de la difusión en Frame Relay tiene dos partes. En primer lugar, el software IOS de Cisco envía copia de las difusiones a través del VC, suponiendo que se haya configurado el router para reenviar estas difusiones necesarias. Si sólo hay unos pocos VCs, esto no es un problema grave. Sin embargo, si hay cientos de VCs que terminan en un router, para cada difusión podrían llegar a enviarse cientos de copias.

Como segunda parte de la solución, el router intenta minimizar el impacto de la primera parte de la solución. El router pone las copias de las difusiones en una cola de salida distinta de la que emplea el tráfico del usuario, para que el usuario no sufra un fuerte retraso cada vez que se duplique una difusión para enviarla a través de todos los VCs. El software IOS de Cisco también se puede configurar para limitar la cantidad de ancho de banda que se utiliza para estas difusiones duplicadas.

Aunque esos problemas de escalabilidad tienen más probabilidades de aparecer en el examen de Enrutamiento CCNP, un breve ejemplo muestra hasta qué punto es significativo el coste adicional de la difusión. Si un router conoce 1000 rutas, utiliza RIP y tiene 50 VCs, se enviarán 1072 MB de actualizaciones RIP cada 30 segundos. Esto supone un promedio de 285 kbps. (El cálculo es como sigue: paquetes RIP de 536 bytes, con 25 rutas por paquete, por 40 paquetes por actualización, enviando copias a través de 50 VCs. 536 * 40 * 50 = 1072 MB por intervalo de actualización. 1.072 * 8 / 30 segundos = 285 kbps.) ¡Es una cantidad enorme de ancho de banda adicional!

La forma de indicar al router cómo reenviar estas difusiones a cada VC se trata en la sección "Configuración y verificación de Frame Relay" del Capítulo 14. Los problemas que están relacionados con la forma de tratar el volumen de estas actualizaciones tienen más probabilidades de ser objeto de los exámenes CCNP y CCIE.

Control de la velocidad y de los descartes en la nube Frame Relay

Este capítulo ya ha examinado los temas más importantes de Frame Relay respecto a la forma en que Frame Relay entrega tramas a través de la red. Esta breve sección final examina unas pocas estrategias que pueden utilizarse para efectuar un ajuste fino del funcionamiento de una red Frame Relay.

El encabezado de Frame Relay contiene tres indicadores de un solo bit que pueden ser utilizados por Frame Relay para controlar lo que sucede dentro de la nube Frame Relay. Estos bits pueden resultar especialmente útiles cuando una o más sedes hacen uso de una velocidad de acceso (la velocidad de reloj del enlace de acceso) que supera con mucho la CIR de un VC. Por ejemplo, si un router tiene un enlace de acceso a Frame Relay de tipo T1, pero sólo dispone de una velocidad de información suscrita (CIR) igual a 128 kbps en un VC que pasa por ese enlace, entonces el router puede enviar a la red Frame Relay muchos más datos que los admitidos por contrato con el proveedor de Frame Relay. Esta sección examina los 3 bits que influyen en la forma en que los switches pueden ayudar a controlar las redes cuando la red se congestiona por estas desigualdades de velocidad, a saber, los bits de Notificación explícita de la congestión (*Forward Explicit Congestion Notification*, FECN), de Notificación de la congestión retrospectiva (*Backward Explicit Congestion Notification*, BECN), y de Posible para descarte (*Discard Eligibility*, DE).

FECN y BECN

Para enfrentarse a aquellos casos en que un router puede enviar más datos que los permitidos por el VC, el IOS ofrece una posibilidad denominada **Conformación de tráfico** (*traffic shaping*), que capacita al router para enviar ciertos paquetes, esperar, enviar más, esperar de nuevo y así sucesivamente. La conformación de tráfico permite al router reducir la tasa global de envío de bits a una velocidad menor que la de acceso, quizá incluso tan baja como la CIR de un VC. Por ejemplo, si se tiene un enlace de acceso T1 y una CIR de 128 kbps, se podría definir la conformación de tráfico para que enviase solamente una media de 256 kbps a través de ese VC. La idea es que el proveedor de Frame Relay probablemente descartará mucho tráfico si el router envía un promedio de datos próximo a T1 a través del VC, que es 12 veces mayor que la CIR en este caso. Sin embargo, quizá el proveedor de Frame Relay no descarte tráfico si la velocidad media es sólo de 256 kbps, que es sólo el doble de la CIR en este caso.

Se puede configurar la conformación de tráfico para que utilice una sola velocidad, o para que se adapte a un cierto rango entre dos ajustes de velocidad. Cuando está configurada para adaptarse entre dos velocidades, si la red no está congestionada, entonces se utiliza la mayor de las dos velocidades; cuando la red está congestionada, el router se adapta a la velocidad inferior.

Para adaptarse a las velocidades cambiantes, los routers necesitan una forma de saber si se está produciendo la congestión: es el momento en que se utilizan los bits FECN y BECN.

FECN y BECN son bits del encabezado Frame Relay. En cualquier punto (bien sea en un router o dentro de la nube Frame Relay) un dispositivo puede activar el bit FECN, indicando que esa trama concreta ha experimentado una congestión. En otras palabras, la congestión existe en la dirección hacia delante de esa trama. En la Figura 13.14, en el Paso 1, el router envía una trama con FECN=0. El switch Frame Relay detecta la congestión y pone FECN=1 en el Paso 2.

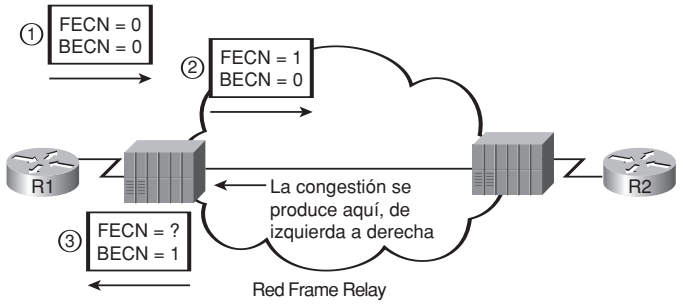


Figura 13.14. Funcionamiento básico de FECN y BECN.

Sin embargo, el objetivo de todo el proceso es conseguir que el router remitente (que es R1 en la figura) vaya más despacio. Por tanto, sabiendo que ha activado FECN en el Paso 2 de la figura, el switch Frame Relay *puede* activar el bit BECN en la próxima trama que vuelva a R1 a través de ese VC, según se muestra en el Paso 3 de la figura. El BECN indica a R1 que se ha producido una congestión en la dirección opuesta, o hacia atrás, respecto a la dirección de la trama. En otras palabras, dice que la congestión se ha producido para la trama enviada por R1 a R2. Entonces R1 puede optar por ir más despacio (o no) dependiendo de cómo esté configurada la conformación de tráfico.

El bit Posible para descarte (*Discard Eligibility*, DE)

Cuando se congestiona la red del proveedor, parece razonable que el proveedor intente descartar las tramas enviadas por aquellos clientes que están produciendo la congestión. Típicamente, los proveedores construyen sus redes de modo que puedan manipular un tráfico mucho mayor que las CIRs acumuladas de todos los VCs. Sin embargo, si uno o más de los clientes abusan de sus derechos mucho más allá de las CIRs contratadas, el proveedor tiene el derecho de descartar únicamente el tráfico enviado por estos clientes.

Los protocolos de Frame Relay definen una forma de suavizar el golpe cuando el cliente envía más de CIR bits por segundo a través de un VC, dando lugar a que el proveedor descarte ciertas tramas. El cliente puede activar el bit DE en algunas tramas. Si los switches del proveedor necesitan descartar tramas como consecuencia de la congestión, los switches pueden descartar las tramas que tengan activado el bit DE. Si el cliente activa el bit DE en las tramas adecuadas, tales como las que correspondan al tráfico menos importante, entonces el cliente puede asegurar que el tráfico importante pase a través de la red Frame Relay, aunque el proveedor tenga que descartar tráfico. Cuando la red del proveedor no está tan congestionada, el cliente puede enviar muchos datos adicionales a través de la red Frame Relay sin que lleguen a ser descartados.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 13.9 especifica estos temas clave y el número de la página en la que se encuentra cada uno.

Tabla 13.9. Temas clave del Capítulo 13.

Tema clave	Descripción	Número de página
Figura 13.1	Figura que muestra varios términos relacionados con una topología Frame Relay.	465
Tabla 13.2	Tabla que enumera términos y definiciones clave de Frame Relay.	466-467
Lista	Dos funciones importantes de la LMI de Frame Relay.	470
Tabla 13.4	Tipos de LMI en Frame Relay y palabras reservadas para la configuración.	471
Figura 13.6	Figura que muestra los encabezados y ubicaciones de los encabezados adicionales de Frame Relay para Cisco y para IETF.	472
Figura 13.9	Figura que muestra el concepto de direccionamiento global en Frame Relay.	475
Lista	Tres opciones de las subredes que se utilizan en una red de Frame Relay.	477
Figura 13.14	Funcionamiento y utilización de los bits FECN y BECN.	484

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD), o por lo menos de la sección de este capítulo, y complete de memoria las tablas y listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas ya completadas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe sus respuestas en el glosario:

ARP inversa, circuito virtual (VC), circuito virtual permanente(PVC), correspondencia de Frame Relay, DCE de Frame Relay, DTE de Frame Relay, Enlace de acceso, identificador de conexión de enlace de datos (DLCI), Interfaz de administración local (LMI), multiacceso sin difusión (NBMA), velocidad de acceso, Velocidad de información suscrita (CIR).

Este capítulo trata los siguientes temas:

Configuración y verificación de Frame Relay: Esta sección muestra la forma de configurar las características obligatorias y opcionales de Frame Relay, con una verificación básica de todas las características.

Resolución de problemas en Frame Relay: Esa sección examina un proceso mediante el cual un ingeniero puede hallar la causa inicial de por qué un router Frame Relay no puede enviar un ping a otro router Frame Relay.

CAPÍTULO 14

Configuración y resolución de problemas de Frame Relay

El Capítulo 13, "Conceptos de Frame Relay", presentaba y explicaba los conceptos principales que subyacen a Frame Relay. Este capítulo muestra la forma de configurar las características en routers Cisco, la forma de verificar que funcionan todas las características, y la forma de resolver problemas relativos al reenvío de paquetes en redes Frame Relay.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de estas ocho preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 14.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

Tabla 14.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
Configuración y verificación de Frame Relay	1-5
Resolución de problemas en Frame Relay	6-8

1. Considere dos routers de Cisco, R1 y R2, que utilizan un servicio Frame Relay. R1 se conecta a un switch que emplea LMI de tipo ANSI T1.617, y R2 se conecta a un switch que emplea ITU Q.933a. ¿Qué palabras reservadas podrían utilizarse en la configuración de R1 y R2 para que las LMIs funcionasen correctamente?
   a. ansi e itu
   b. T1617 y q933
   c. ansi y q933
   d. T1617 e itu
   e. No puede funcionar con dos tipos diferentes.
2. BettyCo tiene cinco sedes, con routers que están conectados a la misma red Frame Relay. Se han definido VCs entre todas las parejas de routers. Betty, que preside la compañía, está dispuesta a despedir a cualquiera que tenga la mala idea de configurar algo que pudiera perfectamente dejarse con su valor predeterminado. ¿Cuáles de los siguientes comandos de configuración, aplicados a una red Frame Relay, harían que el ingeniero fuera despedido?
   a. ip address
   b. encapsulation
   c. lmi-type
   d. frame-relay map
   e. frame-relay inverse-arp
3. WilmaCo tiene ciertos routers conectados a una red Frame Relay. R1 es un router situado en una sede remota, con un único VC que vuelve al cuartel general de WilmaCo. En este momento, la configuración de R1 tiene el aspecto siguiente:

```
interface serial 0/0
  ip address 10.1.1.1
  255.255.255.0 encapsulation frame-relay
```

   Wilma, que preside la compañía, ha oído que las subinterfaces punto a punto están muy bien, y desea cambiar la configuración para que utilice una subinterfaz punto a punto. ¿Cuáles de los comandos siguientes se necesitan para adoptar la nueva configuración?
   a. no ip address
   b. interface-dlci
   c. no encapsulation
   d. encapsulation frame-relay
   e. frame-relay interface-dlci
4. WilmaCo posee otra red, con un router en la sede principal que tiene diez VCs que lo conectan a otras diez sedes remotas. Ahora Wilma piensa que las subinterfaces multipunto son aún mejor que las interfaces punto a punto. La configuración del router de la sede principal tiene el siguiente aspecto en este momento:

```
interface serial 0/0
  ip address 172.16.1.1 255.255.255.0
  encapsulation frame-relay
```

Wilma desea modificar la configuración para utilizar una subinterfaz punto a punto. ¿Cuáles de los comandos siguientes se necesitan para adoptar la nueva configuración? (Nota: los DLCIs de 101 a 110 se están utilizando ya para los diez VCs.)

a. interface-dlci 101 110

b. interface dlci 101-110

c. Diez comandos interface-dlci distintos

d. frame-relay interface-dlci 101 110

e. frame-relay interface dlci 101-110

f. Diez comandos frame-relay interface-dlci distintos

5. ¿Cuál de los siguientes comandos muestra la información aprendida mediante ARP inverso?

a. show ip arp

b. show arp

c. show inverse arp

d. show frame-relay inverse-arp

e. show map

f. show frame-relay map

6. ¿Cuáles de los siguientes son códigos de estado PVC de Frame Relay para los cuales el router envía tramas para el PVC asociado?

a. Up

b. Down

c. Active

d. Inactive

e. Static

f. Deleted

7. El router de la sede central RC tiene un VC que lo conecta a diez routers remotos (de R1 a R10), siendo los DLCIs locales de RC los que tienen los números del 101 al 110, respectivamente. RC ha agrupado los DLCIs 107, 108 y 109 en una sola subinterfaz multipunto S0/0.789, cuyo estado actual es *up*/*up*. ¿Cuáles de las afirmaciones siguientes tienen que ser verdaderas?

a. La interfaz serie 0/0 podría estar en un estado *up*/*down*.

b. El PVC cuyo DLCI es 108 podría hallarse en un estado inactivo.

c. El comando show frame-relay map muestra información de asignación para los tres VCs.

d. Al menos uno de los tres PVCs se encuentra en un estado activo o estático.

8. El router Frame Relay R1 utiliza la interfaz S0/0 para conectarse a un enlace de acceso Frame Relay. La interfaz física se halla en el estado *up/down*. ¿Cuáles de las siguientes podrían ser las causas del problema?
   a. El enlace de acceso tiene un problema físico y no puede pasar bits entre el router y el switch.
   b. El switch y el router utilizan tipos distintos de LMI.
   c. En la configuración del router falta el comando encapsulation frame-relay para la interfaz S0/0.
   d. El router ha recibido un mensaje de estado LMI válido que indicaba que algunos de los DLCIs estaban inactivos.

Temas fundamentales

Este capítulo tiene dos secciones principales. La primera sección examina la configuración de Frame Relay, y además explica varios comandos show. La segunda sección describe la forma de enfocar y resolver los problemas de Frame Relay.

Configuración y verificación de Frame Relay

La configuración de Frame Relay puede ser muy básica o relativamente minuciosa, dependiendo del número de configuraciones predeterminadas que se puedan usar. Por defecto, el IOS de Cisco detecta automáticamente el tipo de LMI y descubre automáticamente la asignación entre DLCI y las direcciones IP de siguiente salto (empleando ARP inverso). Si todos los routers que se utilizan son de Cisco, la opción predeterminada consistente en emplear la configuración de Cisco funciona sin configuración adicional. Si también se diseña la red Frame Relay para emplear una sola subred, se pueden configurar los routers para que utilicen sus interfaces físicas sin subinterfaces; esto hace aún más corta la configuración. De hecho, si se utilizan todos los ajustes predeterminados posibles, la única configuración nueva para Frame Relay, en comparación con las WANs punto a punto, es el comando encapsulation frame-relay.

Las preguntas sobre Frame Relay de los exámenes CCNA pueden ser difíciles por dos razones. En primer lugar, Frame Relay posee una gama de opciones opcionales que se pueden configurar. En segundo lugar, para los ingenieros de redes que ya tienen cierta experiencia con Frame Relay, esa experiencia puede ser con una de entre tres opciones principales de configuración de Frame Relay (física, multipunto o punto a punto), pero el examen abarca las tres opciones. Por tanto, es importante para los exámenes invertir el tiempo necesario para estudiar ejemplos de todas las opciones que se tratan aquí.

Planificación de una configuración de Frame Relay

Los ingenieros tienen que llevar a cabo una cierta planificación antes de saber por dónde hay que empezar la configuración. Aunque casi todas las empresas modernas tienen ya algunas conexiones Frame Relay, cuando se planifican nuevas sedes siempre hay que considerar las cuestiones siguientes, que habrá que comunicar al proveedor de Frame Relay, y que a su vez tienen un cierto impacto sobre las configuraciones Frame Relay del router:

- Definir los sitios físicos que necesitan que se instale un enlace de acceso de Frame Relay, y definir la velocidad de reloj (la velocidad de acceso) que se va a emplear en cada enlace.
- Definir cada VC identificando sus extremos y configurando la CIR.
- Acordar un tipo de LMI (que normalmente vendrá impuesto por el proveedor).

Además, el ingeniero tiene que seleccionar un estilo concreto de configuración basado en lo siguiente. Para estas cuestiones, el ingeniero de la empresa no necesita consultar al proveedor de Frame Relay:

- Seleccionar el esquema de subredes IP: una subred para todos los VCs, una subred para cada VC, o una subred para cada subred de malla completa.
- Decidir si se asignan las direcciones IP a subinterfaces físicas, multipunto o punto a punto.
- Decidir qué VCs necesitan utilizar la encapsulación IETEF en lugar de emplear el valor predeterminado, "cisco." La encapsulación IETF se utiliza típicamente cuando uno de los routers no es de Cisco.

Una vez finalizada la planificación, los pasos de configuración salen directamente de las decisiones tomadas durante la planificación de la red. La lista siguiente resume los pasos de configuración, sobre todo para que sirva como recordatorio de todos los pasos cuando se lleve a cabo la preparación para el examen final. Consulte esta lista en los ejemplos siguientes cuando se le muestre la forma de configurar las distintas opciones. (No hay necesidad de memorizar los pasos; la lista sólo es una herramienta que sirve de ayuda para organizarnos mentalmente respecto a la configuración.)

Paso 1 Configurar la interfaz física para utilizar Frame Relay (subcomando de interfaz `encapsulation frame-relay`).

Paso 2 Configurar una dirección IP para la interfaz o subinterfaz (subcomando `ip address`).

Paso 3 (Opcional) Configurar manualmente el tipo de LMI en cada interfaz serie física (subcomando de interfaz `frame-relay lmi-type`).

Paso 4 (Opcional) Modificar la encapsulación predeterminada para que pase de `cisco` a `ietf` haciendo lo siguiente:

a. Para todos los VCs de la interfaz, añadir la palabra reservada `ietf` al subcomando de interfaz `encapsulation frame-relay`.

b. Para un único VC, añadir la palabra reservada ietf al subcomando de interfaz frame-relay interface-dlci (solo en subinterfaces punto a punto) o al comando frame-relay map.

Paso 5 (Opcional) Si no se va a utilizar (de forma predeterminada) ARP inverso para asignar el DLCI a la dirección IP de siguiente salto, se define una asignación estática empleando el subcomando de subinterfaz frame-relay map ip *dlci dirección-ip* broadcast

Paso 6 En las subinterfaces, se asocia un DLCI (punto a punto) o más (multipunto) con la subinterfaz de una de estas dos maneras:

a. Empleando el subcomando de subinterfaz frame-relay interface-dlci *dlci.*

b. Como efecto secundario de una asignación estática, empleando el subcomando de subinterfaz frame-relay map ip *dlci dirección-ip* broadcast.

El resto de esta sección muestra ejemplos de todos estos pasos de configuración, junto con una descripción de la forma de verificar que la red Frame Relay está operando correctamente.

Una red de malla completa con una subred IP

El primer ejemplo muestra la configuración de Frame Relay más breve posible, que sólo utiliza los dos primeros pasos de la lista de configuración de este capítulo. El diseño del primer ejemplo se basa en las opciones siguientes:

- Instalar un enlace de acceso en tres routers.
- Crear una malla completa de PVCs.
- Utilizar una sola subred (la red de clase C 199.1.1.0) en la red Frame Relay.
- Configurar los routers empleando sus interfaces físicas.

Considere los ajustes predeterminados de LMI, ARP Inverso y encapsulación. Los Ejemplos 14.1, 14.2 y 14.3 muestran la configuración para la red que aparece en la Figura 14.1.

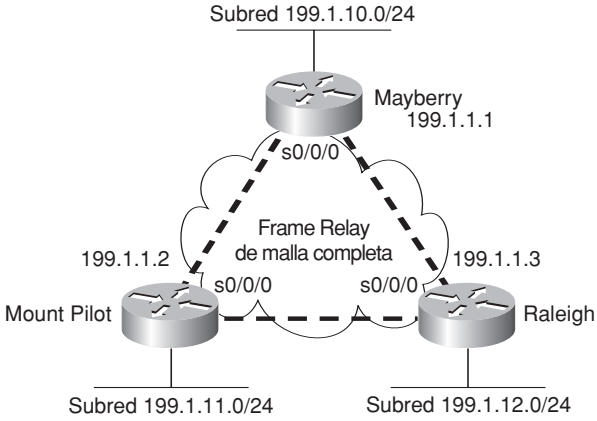


Figura 14.1. Malla completa con direcciones IP.

Ejemplo 14.1. Configuración de Mayberry.

```
interface serial0/0/0
 encapsulation frame-relay
 ip address 199.1.1.1 255.255.255.0
!
interface fastethernet 0/0
 ip address 199.1.10.1 255.255.255.0
!
router eigrp 1
 network 199.1.1.0
 network 199.1.10.0
```

Ejemplo 14.2. Configuración de Mount Pilot.

```
interface serial0/0/0
 encapsulation frame-relay
 ip address 199.1.1.2 255.255.255.0
!
interface fastethernet 0/0
 ip address 199.1.11.2 255.255.255.0
!
router eigrp 1
 network 199.1.1.0
 network 199.1.11.0
```

Ejemplo 14.3. Configuración de Raleigh.

```
interface serial0/0/0
 encapsulation frame-relay
 ip address 199.1.1.3 255.255.255.0
!
interface fastethernet 0/0
 ip address 199.1.12.3 255.255.255.0
!
router eigrp 1
 network 199.1.1.0
 network 199.1.12.0
```

La configuración es sencilla en comparación con los conceptos del protocolo. El comando encapsulation frame-relay indica a los routers que utilicen protocolos de Frame Relay en lugar de emplear el predeterminado, que es HDLC. Obsérvese que las direcciones IP de las interfaces serie de los tres routers están todas ellas en la misma red de clase C. Además, esta sencilla configuración aprovecha los siguientes ajustes predeterminados del IOS:

- Se detecta automáticamente el tipo de LMI.
- La encapsulación (predeterminada) es Cisco en lugar de IETF.

- Los DLCIs de los PVCs se aprenden mediante mensajes de estado de LMI.
- El ARP inverso está habilitado (de forma predeterminada) y se activa cuando se recibe el mensaje de estado que declara que los VCs están activados.

Configuración de la encapsulación y de LMI

En ciertos casos, los valores predeterminados no resultan adecuados. Por ejemplo, es preciso emplear encapsulación IETF si alguno de los routers no es de Cisco. Con el propósito de mostrar una configuración alternativa, supongamos que se añadiesen los requisitos siguientes:

- El router Raleigh requiere encapsulación IETF en ambos VCs.
- El tipo de LMI de Mayberry debería ser ANSI, y no debería utilizarse la autodetección de LMI.

Para modificar estos valores predeterminados deben seguirse los pasos indicados como configuración opcional, concretamente los marcados con los números 3 y 4 en la lista de configuración. Los Ejemplos 14.4 y 14.5 muestran los cambios que se efectuarían en Mayberry y Raleigh.

Ejemplo 14.4. Configuración de Mayberry con los nuevos requisitos.

```
interface serial0/0/0
 encapsulation frame-relay
 frame-relay lmi-type ansi
 frame-relay interface-dlci 53 ietf
 ip address 199.1.1.1 255.255.255.0
! el resto de la configuración no cambia respecto al Ejemplo 14-1.
```

Ejemplo 14.5. Configuración de Raleigh con los nuevos requisitos.

```
interface serial0/0/0
 encapsulation frame-relay ietf
 ip address 199.1.1.3 255.255.255.0

! el resto de la configuración no cambia respecto al Ejemplo 14-3.
```

Estas configuraciones difieren de las anteriores (vistas en los Ejemplos 14.1 y 14.2) en dos aspectos. En primer lugar, Raleigh ha cambiado su encapsulación para ambos PVCs mediante la palabra reservada ietf en el comando encapsulation. Esta palabra reservada se aplica a todos los VCs de la interfaz. Sin embargo, Mayberry no puede cambiar la encapsulación de la misma manera, porque sólo dos de los VCs que terminan en Mayberry necesitan utilizar encapsulación IETF; el otro necesita utilizar la encapsulación Cisco. Por tanto, Mayberry se ve obligado a codificar el comando frame-relay interface-dlci, que hace referencia al DLCI del VC que va a Raleigh, empleando la palabra reserva-

da ietf. Al utilizar este comando, se puede modificar el ajuste de encapsulación para cada VC individual, en lugar de utilizar la configuración de Raleigh, que modifica la encapsulación para todos los VCs.

El segundo cambio de importancia es la configuración de LMI. La configuración de LMI de Mayberry estaría perfectamente sin cambios, porque el uso predeterminado de detección de LMI reconocería a ANSI como tipo de LMI. Sin embargo, al codificar el subcomando de interfaz frame-relay lmi-type ansi, Mayberry tiene que utilizar ANSI, porque este comando no sólo especifica el tipo de LMI, sino que además desactiva la autonegociación del tipo de LMI.

Nota

La configuración LMI se efectúa para cada interfaz física individual, aunque se utilicen subinterfaces, así que el comando frame-relay lmi-type siempre es un subcomando de la interfaz física.

Mount Pilot necesita configurarse mediante un comando frame-relay interface-dlci con la palabra reservada ietf para su VC hacia Raleigh, exactamente igual que Mayberry. Este cambio no se ha mostrado en los ejemplos.

Asignación de direcciones en Frame Relay

La Figura 14.1 ni siquiera intenta reflejar los DLCIs que se utilizan para los VCs. Las configuraciones funcionan según se indica, y francamente, aunque nunca llegáramos a conocer los DLCIs, ¡esta red funcionaría! Sin embargo, para los exámenes, y para trabajos reales relacionados con las redes, es necesario comprender un concepto importante de Frame Relay: la asignación de direcciones de Frame Relay. La Figura 14.2 muestra la misma red, pero esta vez se muestran los valores de DLCI globales.

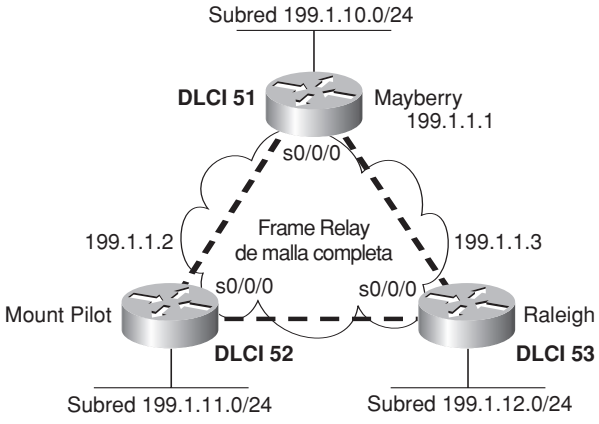


Figura 14.2. Una malla completa, mostrando los DLCIs globales.

El "mapeo" Frame Relay crea una correlación entre una dirección de capa 3 y la correspondiente dirección de capa 2. El concepto es similar a la caché ARP para las interfaces LAN. Por ejemplo, el Protocolo de resolución de direcciones IP (ARP) que se utiliza en las LANs es un ejemplo de mapeo de direcciones de capa 3 a capa 2. Cuando se emplea ARP IP, se conoce la dirección IP de otro dispositivo de la misma LAN, pero no la dirección MAC; cuando finaliza el ARP, se conoce la dirección LAN (de capa 2) de otro dispositivo. Análogamente, los routers que utilizan Frame Relay necesitan un mapeo entre la dirección de capa 3 del router y el DLCI que se emplea para llegar a ese otro router.

Esta sección describe las bases de por qué se necesita una asignación (mapeo) para las conexiones LAN y Frame Relay, centrándose especialmente en Frame Relay. Véase una definición más general de mapeo:

Es la información que define la correlación que hay entre la dirección de capa 3 del router de siguiente salto, y la dirección de capa 2 que se utiliza para llegar a él. El mapeo se necesita en las redes que tienen multiacceso.

Pensar sobre el enrutamiento sirve para hacer más clara la necesidad de un mapeo. Imagine que un host de la Ethernet de Mayberry envía un paquete IP a un host de la Ethernet de Mount Pilot. El paquete llega al router Mayberry a través de la LAN, y Mayberry descarta el encabezado y la información final de Ethernet. Después, Mayberry examina la tabla de enrutamiento, que tiene una entrada correspondiente a una ruta que va hacia 199.1.11.0, interfaz serie de salida Serial 0/0/0, y cuyo router de siguiente salto es 199.1.1.2, que es la dirección IP Frame Relay correspondiente a Mount Pilot.

La próxima decisión que tiene que tomar el router para completar el proceso indica la necesidad de mapeo: ¿qué DLCI debe poner Mayberry en el encabezado de Frame Relay? No hemos configurado los DLCIs. Sin embargo, ¡funcionaría correctamente tal como está configurada la red! Para apreciar la respuesta, considere el Ejemplo 14.6, que muestra comandos importantes para ver la forma en que Mayberry toma una decisión acertada respecto al DLCI.

Ejemplo 14.6. Comandos **show** en Mayberry que muestran la necesidad del mapeo.

```
Mayberry#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

D       199.1.11.0/24 [90/2195456] via 199.1.1.2, 00:00:26, Serial0/0/0
C       199.1.10.0/24 is directly connected, Fastethernet0/0
D       199.1.12.0/24 [90/2185984] via 199.1.1.3, 00:01:04, Serial0/0/0
```

(continúa)

Ejemplo 14.6. Comandos **show** en Mayberry que muestran la necesidad del mapeo *(continuación).*

```
MC      199.1.1.0/24 is directly connected, Serial0/0/0
C       192.68.1.0/24 is directly connected, Fastethernet0/0
C       192.168.1.0/24 is directly connected, Fastethernet0/0

Mayberry#show frame-relay pvc
PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

              Active      Inactive     Deleted      Static
Local           2            0            0           0
Switched        0            0            0           0
Unused          0            0            0           0

DLCI = 52, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0

input pkts 46             output pkts 22           in bytes 2946
out bytes 1794            dropped pkts 0           in FECN pkts 0
in BECN pkts 0            out FECN pkts 0          out BECN pkts 0
in DE pkts 0              out DE pkts 0
out bcast pkts 21         out bcast bytes 1730
pvc create time 00:23:07, last time pvc status changed 00:21:38

DLCI = 53, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0

input pkts 39             output pkts 18           in bytes 2564
out bytes 1584            dropped pkts 0           in FECN pkts 0
in BECN pkts 0            out FECN pkts 0          out BECN pkts 0
in DE pkts 0              out DE pkts 0
out bcast pkts 18         out bcast bytes 1584
pvc create time 00:23:08, last time pvc status changed 00:21:20

Mayberry#show frame-relay map
Serial0/0/0 (up): ip 199.1.1.2 dlci 52(0x34,0xC40), dynamic,
              broadcast,, status defined, active
Serial0/0/0 (up): ip 199.1.1.3 dlci 53(0x35,0xC50), dynamic,
              broadcast,, status defined, active
```

El ejemplo resalta toda la información relacionada en Mayberry para enviar paquetes a la red 199.1.11.0/24 que sale de Mount Pilot. La ruta de Mayberry hacia 199.1.11.0 se refiere a la interfaz serie saliente Serial 0/0/0 y a la dirección 199.1.1.2 como dirección de siguiente salto. El comando show frame-relay pvc muestra dos DLCIs, 52 y 53, y ambos están activados. ¿Cómo conoce Mayberry los DLCIs? A decir verdad, los mensajes de estado de LMI comunican a Mayberry los VCs, los DLCIs asociados y su estado (activo).

¿Qué DLCI debería emplear Mayberry para reenviar el paquete? El resultado del comando show frame-relay map contiene el resultado. Obsérvese la frase resaltada "ip 199.1.1.2 dlci 52" que aparece en la salida. De algún modo, Mayberry ha relacionado a

199.1.1.2, que es la dirección de siguiente salto de la ruta, con el DLCI correcto, que es 52. Por tanto, Mayberry sabe que debe utilizar el DLCI 52 para llegar a la dirección IP de siguiente salto, que es 199.1.1.2.

Mayberry puede utilizar dos métodos para construir el mapeo que se muestra en el Ejemplo 14.6. Uno de ellos emplea un mapeo configurado estáticamente, y el otro emplea un proceso dinámico denominado **ARP Inverso**. Las dos breves secciones siguientes explican los detalles de estas dos opciones.

ARP Inverso

El ARP Inverso crea dinámicamente una asignación entre la dirección de capa 3 (por ejemplo, la dirección IP) y la dirección de capa 2 (el DLCI). El resultado final del ARP Inverso es el mismo que el del ARP IP en una LAN: el router construye una asignación entre una dirección vecina de capa 3 y la dirección correspondiente de capa 2. Sin embargo, el proceso utilizado por ARP Inverso difiere de ARP en una LAN. Una vez que el VC está activado, cada router anuncia su dirección de la capa de red enviando un mensaje de ARP Inverso a través de ese VC. Esto funciona en la forma que se muestra en la Figura 14.3.

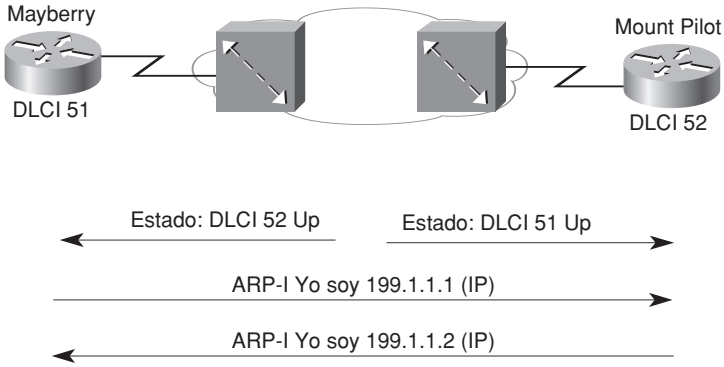


Figura 14.3. Proceso ARP inverso.

Según se muestra en la Figura 14.3, el ARP Inverso anuncia sus direcciones de capa 3 en cuanto la LMI indica que los PVCs están activados. El ARP Inverso comienza aprendiendo la dirección de la capa de enlace de datos de DLCI (mediante mensajes LMI) y después anuncia sus propias direcciones de capa 3 que utilizan ese VC. El ARP inverso está activado de forma predeterminada.

En el Ejemplo 14.6, Mayberry muestra dos entradas diferentes en la salida del comando `show frame-relay map`. Mayberry emplea el ARP inverso para aprender que el DLCI 52 está asignado a la dirección IP de siguiente salto 199.1.1.2 y que el DLCI 53 está asignado a la dirección IP de siguiente salto 199.1.1.3. Curiosamente, Mayberry aprende esta información recibiendo un ARP Inverso procedente de Mount Pilot y de Raleigh, respectivamente.

La Tabla 14.2 resume lo que sucede con ARP Inverso en la red que se muestra en la Figura 14.2.

Tabla 14.2. Mensajes de ARP Inverso para la Figura 14.2.

Router remitente	DLCI cuando se envía la trama	Router receptor	DLCI cuando se recibe la trama	Información que hay en el mensaje ARP Inverso
Mayberry	52	Mount Pilot	51	Soy 199.1.1.1.
Mayberry	53	Raleigh	51	Soy 199.1.1.1.
Mount Pilot	51	Mayberry	52	Soy 199.1.1.2.
Mount Pilot	53	Raleigh	52	Soy 199.1.1.2.
Raleigh	51	Mayberry	53	Soy 199.1.1.3.
Raleigh	52	Mount Pilot	53	Soy 199.1.1.3.

Para comprender el ARP Inverso, considere las dos últimas columnas de la Tabla 14.2. Todos los routers reciben "notificaciones" de ARP Inverso. El mensaje de ARP Inverso contiene la dirección de capa 3 del remitente, y el encabezado de Frame Relay, por supuesto, contiene un DLCI. Estos dos valores se ubican en la caché de ARP Inverso que hay en el router receptor. Por ejemplo, en la tercera fila, Mayberry recibe un ARP Inverso. El DLCI tiene el valor 52 cuando la trama llega a Mayberry y la dirección IP es 199.1.1.2. Esto se añade a la tabla de asignación de Frame Relay que hay en Mayberry, y que se muestra en la parte resaltada del comando `show frame-relay map` en el Ejemplo 14.6.

Mapeo estático en Frame Relay

Se puede configurar estáticamente la misma información de mapeo en lugar de emplear ARP Inverso. En una red de producción, es probable que se utilice directamente ARP Inverso. Para los exámenes es necesario conocer la forma de configurar las sentencias de comandos de mapeo estático. El Ejemplo 14.7 muestra el mapeo estático de Frame Relay para los tres routers que se muestran en la Figura 14.2, junto con la configuración utilizada para inhabilitar el ARP Inverso.

La entrada del comando `frame-relay map` correspondiente a Mayberry, que hace referencia a 199.1.1.2, se utiliza para los paquetes de Mayberry que van a Mount Pilot. Cuando Mayberry crea un encabezado de Frame Relay, con la intención de entregárselo a Mount Pilot, Mayberry tiene que utilizar el DLCI 52. La sentencia `frame-relay map` asocia la dirección IP de Mount Pilot, 199.1.1.2, al DLCI empleado para llegar a Mount Pilot; a saber, el DLCI 52. De forma similar, los paquetes devueltos desde Mount Pilot hasta Mayberry hacen que Mount Pilot utilice su sentencia `map` para hacer referencia a la dirección IP de Mayberry, que es 199.1.1.1. Se necesita el mapeo para todas las direcciones de capa 3 del

Ejemplo 14.7. Comandos **frame-relay map**.

```
Mayberry
interface serial 0/0/0
 no frame-relay inverse-arp
 frame-relay map ip 199.1.1.2 52 broadcast
 frame-relay map ip 199.1.1.3 53 broadcast
```

```
Mount Pilot
interface serial 0/0/0
 no frame-relay inverse-arp
 frame-relay map ip 199.1.1.1 51 broadcast
 frame-relay map ip 199.1.1.3 53 broadcast
```

```
Raleigh
interface serial 0/0/0
 no frame-relay inverse-arp
 frame-relay map ip 199.1.1.1 51 broadcast
 frame-relay map ip 199.1.1.2 52 broadcast
```

siguiente salto en todos los protocolos de capa 3 que se están enrutando. Incluso con una red tan pequeña como esta, el proceso de configuración puede resultar laborioso.

Nota

La palabra reservada broadcast es imprescindible cuando el router necesita enviar difusiones o multidifusiones al router vecino; por ejemplo, para dar soporte a los mensajes de protocolo de enrutamiento tales como los Hellos.

Una red de malla parcial con una subred IP por VC

El segundo ejemplo de red, que está basado en el entorno de la Figura 14.4, utiliza subinterfaces punto a punto. Los Ejemplos del 14.8 al 14.11 muestran la configuración de esta red. Las indicaciones de los comandos se incluyen en el primer ejemplo porque cambian cuando se configuran las subinterfaces.

Una vez más, en esta configuración abundan los ajustes predeterminados, pero algunos valores predeterminados son distintos de los que se emplean cuando se configura la interfaz física. El tipo de LMI se autodetecta, y se emplea la encapsulación de Cisco, exactamente igual que en los ejemplos de malla completa. El ARP Inverso no se necesita realmente en las subinterfaces punto a punto, pero está habilitado de forma predeterminada por si el router que está en el otro extremo del VC necesita utilizar ARP Inverso, como se explicará más adelante en esta sección.

Hay dos comandos nuevos que crean la configuración requerida para subinterfaces punto a punto. En primer lugar, el comando interface serial 0/0/0.1 point-to-point crea la subinterfaz lógica número 1 bajo la interfaz física Serial 0/0/0. El subcomando de subinter-

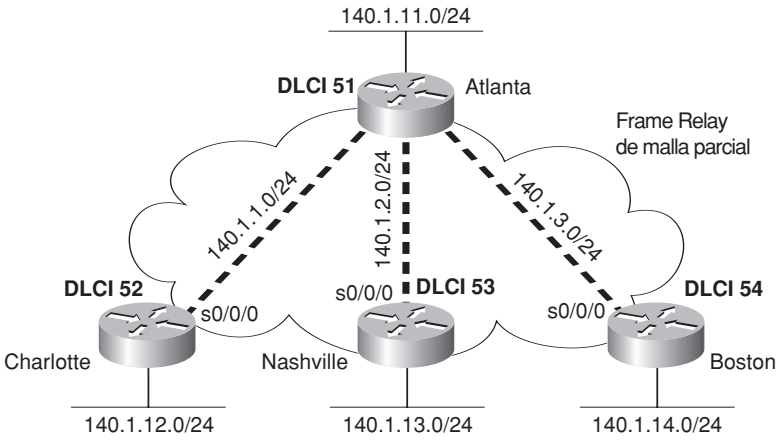


Figura 14.4. Malla parcial con direcciones IP.

Ejemplo 14.8. Configuración de Atlanta.

```
Atlanta(config)#interface serial0/0/0
Atlanta(config-if)#encapsulation frame-relay

Atlanta(config-if)#interface serial 0/0/0.1 point-to-point
Atlanta(config-subif)#ip address 140.1.1.1 255.255.255.0
Atlanta(config-subif)#frame-relay interface-dlci 52

Atlanta(config-fr-dlci)#interface serial 0/0/0.2 point-to-point
Atlanta(config-subif)#ip address 140.1.2.1 255.255.255.0
Atlanta(config-subif)#frame-relay interface-dlci 53

Atlanta(config-fr-dlci)#interface serial 0/0/0.3 point-to-point
Atlanta(config-subif)#ip address 140.1.3.1 255.255.255.0
Atlanta(config-subif)#frame-relay interface-dlci 54

Atlanta(config-fr-dlci)#interface fastethernet 0/0
Atlanta(config-if)#ip address 140.1.11.1 255.255.255.0
```

Ejemplo 14.9. Configuración de Charlotte.

```
interface serial0/0/0
 encapsulation frame-relay
!
interface serial 0/0/0.1 point-to-point
 ip address 140.1.1.2 255.255.255.0
 frame-relay interface-dlci 51
!
interface fastethernet 0/0
 ip address 140.1.12.2 255.255.255.0
```

Ejemplo 14.10. Configuración de Nashville.

```
interface serial0/0/0
 encapsulation frame-relay
!
interface serial 0/0/0.2 point-to-point
 ip address 140.1.2.3 255.255.255.0
 frame-relay interface-dlci 51
!
interface fastethernet 0/0
 ip address 140.1.13.3 255.255.255.0
```

Ejemplo 14.11. Configuración de Boston.

```
interface serial0/0/0
 encapsulation frame-relay
!
interface serial 0/0/0.3 point-to-point
 ip address 140.1.3.4 255.255.255.0
 frame-relay interface-dlci 51
!
interface fastethernet 0/0
 ip address 140.1.14.4 255.255.255.0
```

faz frame-relay interface-dlci indica entonces al router el DLCI (uno solo) que está asociado a esa subinterfaz.

Puede servir de ayuda un ejemplo del funcionamiento del comando frame-relay interface-dlci. Considere el router Atlanta de la Figura 14.4. Atlanta recibe mensajes LMI a través de Serial0/0/0 que indican que hay tres PVCs, cuyos DLCIs son respectivamente 52, 53 y 54, que están activados. ¿Qué PVC corresponde a qué subinterfaz? El software IOS de Cisco necesita asociar el PVC correcto con la subinterfaz correcta. Esto se logra mediante el comando frame-relay interface-dlci.

Los números de subinterfaz no tienen por qué coincidir en el router que se halla al otro extremo del PVC, y tampoco tiene que coincidir el número de DLCI. En este ejemplo, se han numerado las subinterfaces para que fuesen más fáciles de recordar. En la vida real, resulta útil codificar parte de la información relativa al esquema de numeración de red en el número de la subinterfaz. Por ejemplo, una compañía podría codificar el ID de circuito de la portadora en el número de la subinterfaz, para que el personal de mantenimiento pudiera hallar la información correcta que debe comunicarse a la compañía de telecomunicaciones cuando se resuelven problemas en el enlace. Hay muchos sitios que utilizan el DLCI como número de subinterfaz. Por supuesto, la información útil para la resolución de problemas, como el DLCI, el nombre del router que hay al otro extremo del VC y demás, se podría configurar también como texto empleando el comando description. Sea como fuere, no hay requisitos que exijan que los números de subinter-

faz coincidan. Este ejemplo se limita a igualar el número de subinterfaz al tercer octeto de la dirección IP.

Asignación de un DLCI a una subinterfaz particular

Según se ha mencionado en la lista de configuración que hay al principio de la sección "Configuración y verificación de Frame Relay", cuando se configuran subinterfaces los DLCIs tienen que asociarse a las subinterfaces de dos formas posibles. Los Ejemplos del 14.8 al 14.11 mostraban la forma de asociar los DLCIs empleando el subcomando de subinterfaz `frame-relay interface-dlci`. La configuración alternativa consistiría en emplear el comando `frame-relay map` como subcomando de una subinterfaz. Este comando haría dos cosas: asociaría un DLCI a la subinterfaz y configuraría estáticamente una asignación de la dirección IP del siguiente salto de capa 3 a este DLCI. Por ejemplo, en Atlanta, se podría utilizar el comando `frame-relay map ip 140.1.1.2 52 broadcast` en la interfaz S0/0/0.1, sustituyendo al comando `frame-relay interface-dlci 52` en el Ejemplo 14.8.

El router desactiva el ARP Inverso en una subinterfaz cuando se aplica el comando `frame-relay map`. Por tanto, cuando se utilizan mapas estáticos en el router de un extremo de un VC, hay que tener en cuenta que el router situado en el otro extremo del VC no recibirá mensajes de ARP Inverso, y quizá sea necesario configurarlo mediante el comando `frame-relay map`.

Comentarios sobre el direccionamiento global y local

Cuando se pasan los exámenes CCNA de Cisco, si una figura de una pregunta muestra tres o más routers, debería resultar sencillo decidir si la figura implica valores locales o globales de DLCI. Por ejemplo, la Figura 14.4 muestra una sede central con tres PVCs, cada uno de los cuales llega a una sede remota. Sin embargo, sólo se muestra un DLCI junto al router de la sede central, lo cual implica el uso de un direccionamiento global. Si se utilizasen DLCIs locales, la figura tendría que mostrar un DLCI para cada PVC junto al router de la sede central.

En aquellos casos en que una figura de una cuestión sólo muestra dos routers, la figura podría no implicar si se utiliza direccionamiento DLCI global o local. En estos casos, hay que buscar pistas en la pregunta, en las respuestas y en cualquier posible configuración. Las mejores pistas están relacionadas con el hecho siguiente:

> En cualquier router dado, en la configuración o en los comandos `show` sólo hay valores locales de DLCI.

Considere de nuevo la Figura 14.4 junto con los Ejemplos del 14.8 al 14.11. La figura muestra DLCIs globales, con el DLCI 51 junto al router Atlanta. Sin embargo, los comandos `frame-relay interface-dlci` del router Atlanta (Ejemplo 14.8) y los comandos `show` de Atlanta que hay en el (próximo) Ejemplo 14.12 muestran los DLCIs 52, 53 y 54. Aunque la Figura 14.4 pone de manifiesto que se utiliza un direccionamiento global, aunque sólo se hubieran mostrado dos routers, los comandos `show` y los comandos de configuración podrían haber servido de ayuda para identificar los DLCIs correctos que hay que emplear.

Verificación de Frame Relay

El Ejemplo 14.12 muestra la salida de los comandos EXEC más comunes del software IOS de Cisco para Frame Relay que sirven para monitorizar Frame Relay, tal como se han ejecutado en el router Atlanta.

Ejemplo 14.12. Salida de los comandos EXEC en Atlanta.

```
Atlanta#show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

              Active        Inactive     Deleted      Static
 Local          3             0            0           0
 Switched       0             0            0           0
 Unused         0             0            0           0
DLCI = 52, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.1

 input pkts 843            output pkts 876          in bytes 122723
 out bytes 134431          dropped pkts 0           in FECN pkts 0
 in BECN pkts 0            out FECN pkts 0          out BECN pkts 0
 in DE pkts 0              out DE pkts 0
 out bcast pkts 876        out bcast bytes 134431
 pvc create time 05:20:10, last time pvc status changed 05:19:31
 --More--
DLCI = 53, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.2

 input pkts 0              output pkts 875          in bytes 0
 out bytes 142417          dropped pkts 0           in FECN pkts 0
 in BECN pkts 0            out FECN pkts 0          out BECN pkts 0
 in DE pkts 0              out DE pkts 0
 out bcast pkts 875        out bcast bytes 142417
 pvc create time 05:19:51, last time pvc status changed 04:55:41
 --More--
DLCI = 54, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.3

 input pkts 10             output pkts 877          in bytes 1274
 out bytes 142069          dropped pkts 0           in FECN pkts 0
 in BECN pkts 0            out FECN pkts 0          out BECN pkts 0
 in DE pkts 0              out DE pkts 0
 out bcast pkts 877        out bcast bytes 142069
 pvc create time 05:19:52, last time pvc status changed 05:17:42

Atlanta#show frame-relay map
Serial0/0/0.3 (up): point-to-point dlci, dlci 54(0x36,0xC60), broadcast
          status defined, active
Serial0/0/0.2 (up): point-to-point dlci, dlci 53(0x35,0xC50), broadcast
          status defined, active
```

(continúa)

Ejemplo 14.12. Salida de los comandos EXEC en Atlanta *(continuación)*.

```
Serial0/0/0.1 (up): point-to-point dlci, dlci 52(0x34,0xC40), broadcast
          status defined, active

Atlanta#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data

Serial0/0/0(out): StEnq, myseq 163, yourseen 161, DTE up
datagramstart = 0x45AED8, datagramsize = 13
FR encap = 0xFCF10309
00 75 01 01 01 03 02 A3 A1

Serial0/0/0(in): Status, myseq 163
RT IE 1, length 1, type 1
KA IE 3, length 2, yourseq 162, myseq 163
```

El comando show frame-relay pvc muestra información útil para la administración. Por ejemplo, los contadores de paquetes de cada VC, y los contadores de FECN y BECN pueden resultar especialmente útiles. De forma similar, la comparación de los paquetes y bytes enviados a través de un router con los contadores de lo que se recibe en el otro extremo del VC es también bastante útil. Esto refleja el número de paquetes y bytes perdidos en la nube Frame Relay. Además, el estado de PVC es un excelente punto de partida para la resolución de problemas.

El comando show frame-relay map muestra información de asignación. Con el ejemplo anterior de una red de malla completa, en el cual la configuración no utilizaba subinterfaces, se mostraba una dirección de capa 3 junto a cada DLCI. En este ejemplo, se muestra un DLCI en cada entrada, pero no se mencionan las direcciones correspondientes de la capa 3. El objetivo primordial del mapeo es establecer una correlación entre una dirección de capa 3 y una dirección de capa 2, pero en la salida del comando show frame-relay map no hay una dirección de capa 3. La razón es que la información está almacenada en otro lugar. Las subinterfaces requieren utilizar el comando de configuración frame-relay interface-dlci. Como las subinterfaces son punto a punto, cuando una ruta señala una sola subinterfaz, el DLCI que debe emplearse para enviar tramas está sugerido por la configuración. El mapeo a través de ARP Inverso o de sentencias estáticas frame-relay map sólo es necesario cuando hay más de dos VCs que terminan en la interfaz o subinterfaz, porque esos son los únicos casos en que se podría producir una confusión relativa al DLCI que hay que utilizar.

La salida de debug frame-relay lmi muestra información relativa al envío y recepción de peticiones LMI. El switch envía el mensaje de estado, y el DTE (el router) envía la petición de estado. El ajuste predeterminado cuando se utiliza el software IOS de Cisco consiste en enviar, y en esperar recibir, estos mensajes de estado. El comando no keepalive del software IOS sirve para inhabilitar el uso de mensajes LMI de estado. A diferencia de otras interfaces, los mensajes *keepalive* de Cisco no van de router a router a través de Frame Relay. En

lugar de hacer esto, se utilizan simplemente para detectar si el router tiene conectividad con su switch Frame Relay local.

Una red de malla parcial con partes de malla completa

También se pueden utilizar subinterfaces multipunto para una configuración de Frame Relay. Este último ejemplo de red, basado en la red que se muestra en la Figura 14.5, utiliza subinterfaces multipunto y punto a punto. Los Ejemplos del 14.13 al 14.17 muestran la configuración correspondiente a esta red. La Tabla 14.3 resume las direcciones y subinterfaces utilizadas.

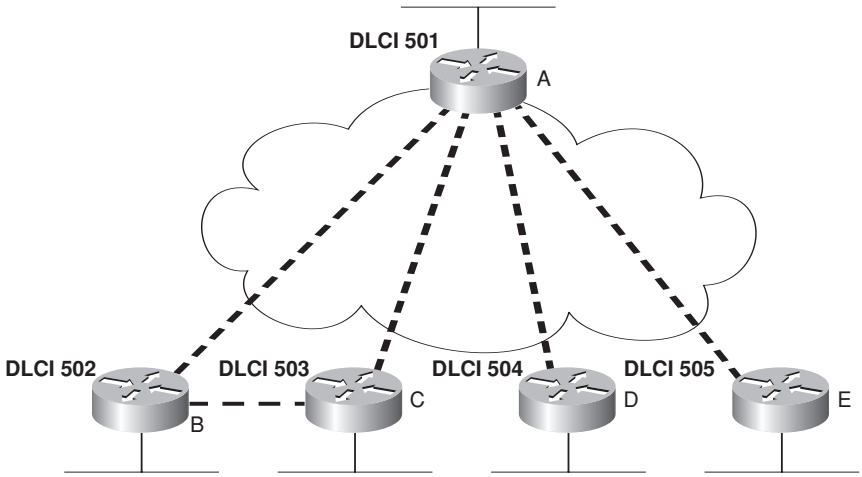


Figura 14.5. Híbrido de malla completa y parcial.

Ejemplo 14.13. Configuración del router A.

```
interface serial0/0/0
 encapsulation frame-relay
!
interface serial 0/0/0.1 multipoint
 ip address 140.1.1.1 255.255.255.0
 frame-relay interface-dlci 502
 frame-relay interface-dlci 503
!
interface serial 0/0/0.2 point-to-point
 ip address 140.1.2.1 255.255.255.0
 frame-relay interface-dlci 504
!
```

(continúa)

Ejemplo 14.13. Configuración del router A *(continuación).*

```
interface serial 0/0/0.3 point-to-point
 ip address 140.1.3.1 255.255.255.0
 frame-relay interface-dlci 505
```

Ejemplo 14.14. Configuración del router B.

```
interface serial0/0/0
 encapsulation frame-relay
!
interface serial 0/0/0.1 multipoint
 ip address 140.1.1.2 255.255.255.0
 frame-relay interface-dlci 501
 frame-relay interface-dlci 503
```

Ejemplo 14.15. Configuración del router C.

```
interface serial0/0/0
 encapsulation frame-relay
!
interface serial 0/0/0.1 multipoint
 ip address 140.1.1.3 255.255.255.0
 frame-relay interface-dlci 501
 frame-relay interface-dlci 502
```

Ejemplo 14.16. Configuración del router D.

```
interface serial0/0/0
 encapsulation frame-relay
!
interface serial 0/0/0.1 point-to-point
 ip address 140.1.2.4 255.255.255.0
 frame-relay interface-dlci 501
```

Ejemplo 14.17. Configuración del router E.

```
interface serial0/0/0
 encapsulation frame-relay
!
interface serial 0/0/0.1 point-to-point
 ip address 140.1.3.5 255.255.255.0
 frame-relay interface-dlci 501
```

Las subinterfaces multipunto funcionan especialmente bien cuando se tiene una malla completa que une a un conjunto de routers. En los Routers A, B y C, se utiliza una subinterfaz multipunto para la configuración que hace referencia a los otros dos routers, porque se puede pensar que estos tres routers forman un subconjunto que es una malla completa de la red.

Tabla 14.3. Direcciones IP con subinterfaces punto a punto y multipunto.

Router	Subred	Dirección IP	Tipo de subinterfaz
A	140.1.1.0/24	140.1.1.1	Multipunto
B	140.1.1.0/24	140.1.1.2	Multipunto
C	140.1.1.0/24	140.1.1.3	Multipunto
A	140.1.2.0/24	140.1.2.1	Punto a punto
D	140.1.2.0/24	140.1.2.4	Punto a punto
A	140.1.3.0/24	140.1.3.1	Punto a punto
E	140.1.3.0/24	140.1.3.5	Punto a punto

El término multipunto significa simplemente que hay más de un VC, así que se puede enviar y recibir a y desde más de un VC a través de la subinterfaz. Al igual que las subinterfaces punto a punto, las subinterfaces multipunto utilizan el comando frame-relay interface-dlci. Obsérvese que en este caso hay dos comandos para cada subinterfaz multipunto, porque cada uno de los dos PVCs asociados a esta subinterfaz tiene que estar identificado como utilizado con esa subinterfaz.

El Router A es el único router que emplea simultáneamente subinterfaces multipunto y punto a punto. En la interfaz multipunto Serial0/0/0.1 del Router 1, se muestran DLCIs para los Routers B y C. En las otras dos subinterfaces del Router A, que son punto a punto, sólo es necesario mostrar un DLCI. De hecho, sólo se admite un comando frame-relay interface-dlci en las subinterfaces punto a punto, porque sólo se permite un VC. Por lo demás, las configuraciones entre los dos tipos son similares.

No se necesitan sentencias de asignación para las configuraciones que se muestran en los Ejemplos del 14.13 al 14.17, porque está habilitado el ARP Inverso en las subinterfaces multipunto de forma predeterminada. Nunca se necesita mapeo para las subinterfaces punto a punto, porque el único DLCI asociado a la interfaz está configurado estáticamente mediante el comando frame-relay interface-dlci.

El Ejemplo 14.18 muestra otro comando show frame-relay map, que ofrece la información de mapeo aprendida mediante ARP Inverso para la subinterfaz multipunto. Obsérvese que ahora la salida incluye las direcciones de capa 3, mientras que ese mismo comando, cuando se utilizan subinterfaces punto a punto (en el Ejemplo 14.12) no lo hacía. La razón es que las rutas podrían hacer referencia a una dirección IP de siguiente salto que fuera alcanzable a través de una interfaz multipunto, pero como hay más de un DLCI asociado a la interfaz, el router necesita información de mapeo para asociar la dirección IP de siguiente salto con el DLCI correcto.

Los mensajes relativos a ARP Inverso que aparecen en la salida de debug frame-relay events no resultan tan evidentes. Un ejercicio sencillo consiste en buscar la versión hexadeci-

mal de las direcciones IP en la salida. Esas direcciones están resaltadas en el Ejemplo 14.18. Por ejemplo, los 4 primeros bytes de 140.1.1.1 son 8C 01 01 01 en hexadecimal. Este campo comienza en el lado izquierdo del resultado, así que resulta fácil de reconocer.

Ejemplo 14.18. Asignaciones de Frame Relay y ARP Inverso en el Router C.

```
RouterC#show frame-relay map
Serial0/0/0.1 (up): ip 140.1.1.1 dlci 501(0x1F5,0x7C50), dynamic,
              broadcast,, status defined, active
Serial0/0/0.1 (up): ip 140.1.1.2 dlci 502(0x1F6,0x7C60), dynamic,
              broadcast,, status defined, active

RouterC#debug frame-relay events
Frame Relay events debugging is on

RouterC#configure terminal
Enter configuration commands, one per line. End with Ctrl-Z.
RouterC(config)#interface serial 0/0/0.1
RouterC(config-subif)#shutdown
RouterC(config-subif)#no shutdown
RouterC(config-subif)#^Z
RouterC#

Serial0/0/0.1: FR ARP input
Serial0/0/0.1: FR ARP input
Serial0/0/0.1: FR ARP input
datagramstart = 0xE42E58, datagramsize = 30
FR encap = 0x7C510300
80 00 00 00 08 06 00 0F 08 00 02 04 00 09 00 00
8C 01 01 01 7C 51 8C 01 01 03

datagramstart = 0xE420E8, datagramsize = 30
FR encap = 0x7C610300
80 00 00 00 08 06 00 0F 08 00 02 04 00 09 00 00
8C 01 01 02 7C 61 8C 01 01 03
```

Resolución de problemas en Frame Relay

Frame Relay posee muchas opciones y posibilidades que se pueden configurar. Tanto en la vida real como en los exámenes, la resolución de problemas de Frame Relay suele significar que es preciso examinar las configuraciones de todos los routers y asegurarse de que esas configuraciones cumplen los requisitos. Los tipos de LMI tienen que coincidir o detectarse automáticamente, es preciso que se hayan asociado los valores correctos de DLCI con cada subinterfaz, etcétera. Por tanto, para estar bien preparado para los exámenes de CCNA, se deben revisar y memorizar las muchas opciones de configuración que ofrece Frame Relay, y lo que significa cada una de ellas.

Sin embargo, los exámenes pueden contener cuestiones de Frame Relay que requieran resolver un problema sin examinar la configuración. La segunda de las secciones principales del capítulo examina la resolución de problemas de Frame Relay, haciendo hincapié en la forma de utilizar los comandos show, junto con los síntomas de los problemas, para aislar la causa inicial del problema.

Proceso sugerido para la resolución de problemas de Frame Relay

Para aislar un problema de Frame Relay, el proceso debería comenzar con algunos *pings*. Idealmente, los *pings* desde un host de usuario final de una LAN hasta otro host de una LAN remota pueden determinar rápidamente si la red puede cumplir en este momento su objetivo principal, consistente en enviar paquetes entre computadoras. Si falla ese ping, un ping desde un router hasta la dirección IP de Frame Relay del otro router es el paso siguiente. Si funciona ese ping, pero ha fallado el ping del usuario, el problema tiene que ver con temas de la capa 3, y la resolución de problemas asociados a esas cuestiones se ha tratado adecuadamente en los Capítulos 7 y 11. Sin embargo, si falla un ping desde un router a la dirección IP Frame Relay de otro router, lo más probable es que el problema esté relacionado con la red Frame Relay.

Esta sección se centra en la resolución de problemas cuando un router Frame Relay no puede enviar un ping a la dirección IP Frame Relay de otro router. En ese momento, el ingeniero debería hacer un ping a las direcciones IP de todos los demás routers que están en el otro extremo de cada VC para determinar lo siguiente:

¿Fallan los *pings* para las direcciones IP Frame Relay de todos routers remotos, o fallan algunos y funcionan otros?

Por ejemplo, la Figura 14.6 muestra un ejemplo de red Frame Relay que se utilizará en los ejemplos restantes de este capítulo. Si R1 intentase hacer un ping a la dirección IP Frame Relay de R2 (que en este caso es 10.1.2.2) y fallase, la pregunta siguiente es si los *pings* de R1 a R3 (10.1.34.3) y a R4 (10.1.34.4) funcionan o no.

Este capítulo organiza sus explicaciones sobre la forma de resolver problemas de Frame Relay basándose en este primer paso para aislar el problema. La lista siguiente resume las acciones más importantes, y cada uno de sus pasos se examina, por orden, después de la lista.

Si los *pings* de un router Frame Relay fallan para todos los routers remotos cuyos VCs comparten un solo enlace de acceso, haga lo siguiente:

Paso 1 Busque problemas de la capa 1 en el enlace de acceso que media entre el router y el switch Frame Relay local (para todos los routers).

Paso 2 Busque problemas de la capa 2 en el enlace de acceso, y especialmente los relativos a encapsulación y a LMI.

Después de resolver los posibles problemas que aparecen en los dos primeros pasos, o si las pruebas hechas inicialmente con ping han mostrado que el router Frame Relay pue-

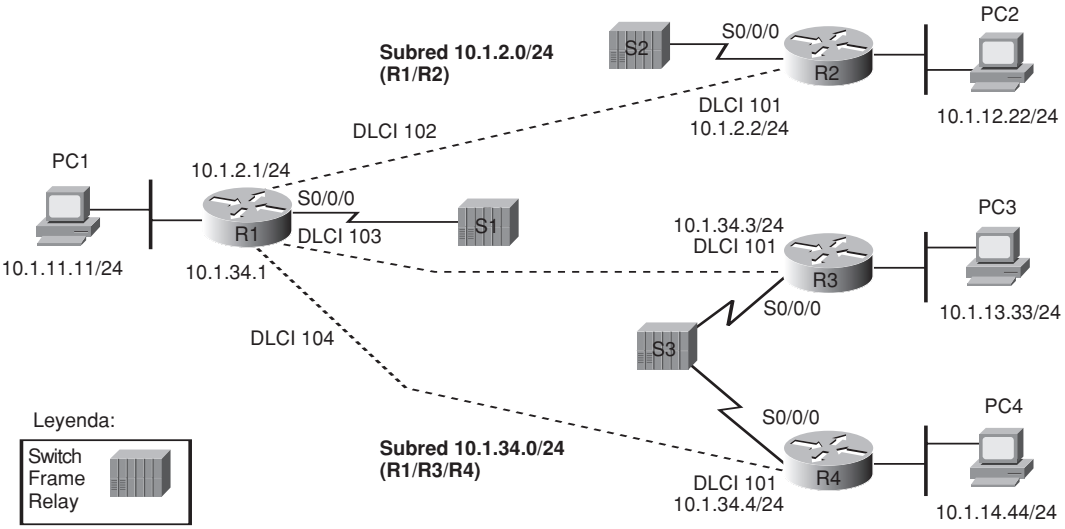


Figura 14.6. Ejemplo de red Frame Relay para los ejemplos de resolución de problemas.

de hacer ping a algunos de los routers Frame Relay cuyos VCs comparten un único enlace de acceso, pero no a todos, siga estos pasos:

Paso 3 Busque problemas de PVC basándose en el estado del PVC y en el estado de la subinterfaz.

Paso 4 Busque problemas de las capas 2/3, tanto con mapeo estático como con mapeo dinámico (ARP inverso).

Paso 5 Busque problemas de las capas 2/3 relacionados con desigualdades entre las encapsulaciones de ambos extremos (cisco o ietf).

Paso 6 Busque otros problemas de la capa 3, incluyendo faltas de coincidencia en las subredes.

El resto del capítulo explica algunos de los detalles de cada paso de este proceso sugerido para la resolución de problemas.

Problemas de capa 1 relativos al enlace de acceso (Paso 1)

Si la interfaz física de un router que se usa para el enlace de acceso Frame Relay no se encuentra en un estado "*up*/*up*", el router no puede enviar tramas a través del enlace. Si la interfaz tiene un estado de línea *down* (que es el primer código de estado de interfaz), lo más probable es que la interfaz tenga un problema de capa 1.

Desde una perspectiva de la capa 1, un enlace de acceso Frame Relay es meramente una línea alquilada que une un router con un switch Frame Relay. Como tal, para este

enlace existen exactamente los mismos problemas que para una línea alquilada punto a punto. Como las posibles causas iniciales y los pasos para la resolución de problemas son idénticos a lo que se debería hacer en una línea alquilada, consulte la sección "Resolución de problemas de capa 1" del Capítulo 12 si desea más información relativa a este paso.

Problemas de capa 2 relativos al enlace de acceso (Paso 2)

Si el estado de línea de la interfaz física del router es *up*, pero el estado de protocolo de línea (que es el segundo código de estado) es *down*, normalmente el enlace tiene un problema de capa 2 entre el router y el switch Frame Relay local. En las interfaces Frame Relay, el problema suele estar relacionado con el comando encapsulation o con la LMI de Frame Relay.

El problema potencial con el comando encapsulation es muy fácil de comprobar. Si la configuración de la interfaz serie de un router omite el subcomando encapsulation frame-relay, pero el enlace de acceso físico funciona, entonces la interfaz física queda en un estado *up*/*down*. Si la configuración no está disponible, se puede utilizar el comando show interfaces para determinar el tipo de encapsulación que se ha utilizado, y que se muestra en las primeras líneas de la salida del comando.

El otro problema potencial está relacionado con la LMI. Los mensajes de estado LMI fluyen en ambas direcciones entre el router (el DTE) y el switch Frame Relay (el DCE) con dos propósitos principales:

- Que el DCE informe al DTE acerca del DLCI de cada VC y de su estado.
- Para proporcionar una función de actividad de tal modo que el DTE y el DCE puedan determinar fácilmente si el enlace de acceso ya no admite tráfico.

El router pone el enlace físico en el estado *up*/*down* cuando el enlace funciona físicamente pero el router deja de oír mensajes LMI procedentes del switch. Cuando la interfaz no se encuentra en un estado *up*/*up*, el router no intenta enviar paquetes IP a través de la interfaz, así que en esa situación deberían fallar todos los *pings*.

Es posible que un router deje de recibir mensajes LMI del switch tanto por razones legítimas como por errores. El propósito legítimo normal de la función de actividad de LMI es que si el enlace tiene problemas y no puede pasar datos el router puede notar la pérdida de mensajes de actividad y desactivar el enlace. Esto permite al router emplear una ruta alternativa, suponiendo que exista una ruta alternativa. Sin embargo, un router podría dejar de recibir mensajes LMI y desactivar la interfaz como consecuencia de los errores siguientes:

- Inhabilitar LMI en el router (mediante el subcomando no keepalive aplicado a la interfaz física), pero dejarlo habilitado en el switch, o a la inversa.
- Configurar distintos tipos de LMI en el router (mediante el subcomando frame-relay lmi-type *tipo* en la interfaz física) y en el switch.

Es fácil comprobar tanto la encapsulación como la LMI empleando el comando show frame-relay lmi. Este comando sólo muestra resultados para las interfaces que se hayan configurado con el comando encapsulation frame-relay, así que se puede confirmar rápidamente si se ha aplicado el comando encapsulation frame-relay en las interfaces serie correctas. Este comando también muestra el tipo de LMI que se utiliza en el router, y muestra contadores para el número de mensajes LMI que se envían y se reciben. El Ejemplo 14.19 muestra un ejemplo desde el router R1 de la Figura 14.6.

Ejemplo 14.19. Comando **show frame-relay lmi** en R1.

```
R1#show frame-relay lmi

LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE = ANSI
 Invalid Unnumbered info 0            Invalid Prot Disc 0
 Invalid dummy Call Ref 0             Invalid Msg Type 0
 Invalid Status Message 0             Invalid Lock Shift 0
 Invalid Information ID 0             Invalid Report IE Len 0
 Invalid Report Request 0             Invalid Keep IE Len 0
 Num Status Enq. Sent 122             Num Status msgs Rcvd 34
 Num Update Status Rcvd 0             Num Status Timeouts 88
 Last Full Status Req 00:00:04        Last Full Status Rcvd 00:13:24
```

Para este ejemplo, el router R1 se ha configurado estáticamente mediante el subcomando de interfaz frame-relay lmi-type ansi, con el switch S1 empleando todavía el tipo cisco de LMI. Cuando se cambia la configuración de LMI, el router y el switch habían intercambiado 34 mensajes LMI (de tipo cisco). Después del cambio, el contador de R1 que contiene el número de mensajes de consulta de estado ha seguido subiendo (122 cuando se capturó la salida del comando show frame-relay lmi), pero el contador de número de mensajes de estado LMI recibidos procedentes del switch quedó en 34. Justamente debajo del contador está el número de veces que se agota el tiempo, que denota el número de veces que el router esperaba recibir un mensaje periódico de LMI procedente del switch, pero que no ha recibido. En este caso, el router seguía recibiendo mensajes LMI, pero no eran mensajes ANSI LMI, así que el router no los comprendía o reconocía.

Si el uso repetido del comando show frame-relay lmi muestra que el número de mensajes de estado recibidos no varía, entonces la causa probable, salvo un enlace que realmente no funcione, es que los tipos de LMI no coincidan. La mejor solución consiste en admitir la autodetección de LMI, empleando el subcomando no frame-relay lmi-type *tipo* en la interfaz física, o alternativamente, configurar el mismo tipo de LMI que esté siendo utilizado por el switch.

Si se estudia la situación y se corrigen los problemas que puedan hallarse en los Pasos 1 y 2 en todos los routers Frame Relay conectados, entonces todas las interfaces físicas de los enlaces de acceso de todos los routers deberían encontrarse en el estado *up*/*up*. Los cuatro últimos pasos examinan los problemas aplicables a PVCs y vecinos individuales.

Problemas y estado de los PVCs (Paso 3)

La meta de este paso del proceso de resolución de problemas es descubrir el DLCI del PVC que se emplea para llegar a un determinado vecino, y averiguar después si está funcionando el PVC. Para determinar el PVC correcto, especialmente si se dispone de poca documentación o configuración, es preciso comenzar en el comando ping fallido. El comando ping identifica la dirección IP del router vecino. Basándose en la dirección IP del vecino, unos cuantos comandos show pueden relacionar la dirección IP del vecino con la subred conectada asociada, la subred conectada con la interfaz del router local, y la interfaz del router local con los posibles DLCIs. Además, la información de mapeo de Frame Relay puede identificar al PVC concreto. Aunque este libro ha tratado todos los comandos que se utilizan para obtener estas informaciones, la lista siguiente resume los pasos que se nos llevan de la dirección IP del vecino al DLCI local correcto que se emplea para enviar tramas a ese vecino:

Paso 3a Determine la dirección IP y la máscara de todas las interfaces y subinterfaces de Frame Relay (show interfaces, show ip interface brief), y calcule las subredes conectadas.

Paso 3b Compare la dirección IP del comando ping fallido, y seleccione la interfaz o subinterfaz cuya subred conectada esté en la misma subred.

Paso 3c Determine el o los PVCs asignados a esa interfaz o subinterfaz (show frame-relay pvc).

Paso 3d Si hay más de un PVC asignado a la interfaz o subinterfaz, determine qué PVC se utiliza para llegar a un determinado vecino (show frame-relay map).

Nota

Como recordatorio, las listas de este tipo intentan ser una referencia cómoda cuando se lee el capítulo. Es fácil buscar la lista cuando está uno estudiando y desea recordar una parte concreta de la forma en que se ataca un determinado problema. No es necesario memorizar la lista, sólo practicar con ella hasta asimilar la información.

Los pasos 3a, 3b, 3c y 3d descubren el PVC correcto que hay que examinar. Una vez obtenido, el Paso 3 del proceso sugerido para la resolución de problemas interpreta el estado de ese PVC y de la interfaz o subinterfaz asociada, para determinar la causa de los posibles problemas.

Esta sección examina con más detalle un ejemplo en que R1 no puede hacer un ping a la dirección IP Frame Relay asociada a R2. Antes de centrarnos en el proceso seguido para determinar qué VC se emplea, resulta útil examinar la respuesta final, así que la Figura 14.7 muestra algunos detalles. Para este ejemplo, en R1 falla el comando ping 10.1.2.2.

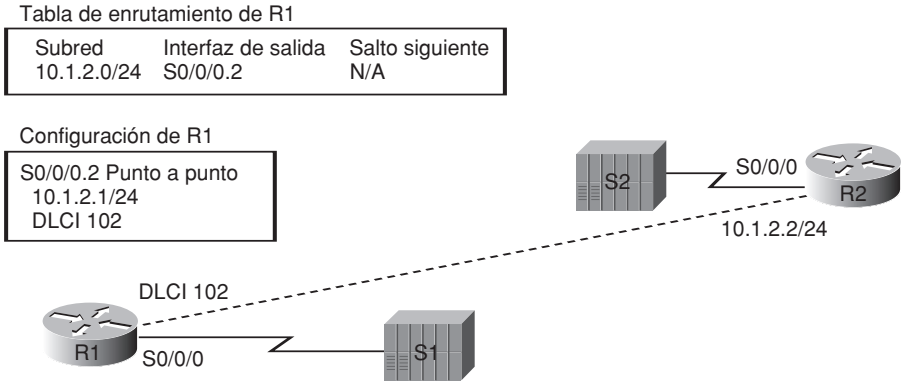


Figura 14.7. Detalles de configuración relacionados con el fallo del comando **ping 10.1.2.2** en R1.

Búsqueda de la subred conectada y de la interfaz de salida (Pasos 3a y 3b)

Los dos primeros pasos intermedios para buscar el PVC (el DLCI realmente) de R1 que lo conecta a R2 (pasos intermedios 3a y 3b) deberían ser relativamente sencillos suponiendo que ya se hayan estudiado las Partes II y III del libro. Siempre que se hace un ping a la dirección IP Frame Relay del router vecino, esa dirección IP debería estar en una de las subredes que también está conectada al router local. Para averiguar la interfaz utilizada en un router local cuando se reenvían paquetes al router remoto, sólo hay que buscar la subred común conectada.

En este ejemplo, con R1 que hace un ping a 10.1.2.2, el Ejemplo 14.20 muestra unos pocos comandos que confirman que la subinterfaz S0/0/0.2 de R1 está conectada a la subred 10.1.2.0/24, que incluye la dirección IP 10.1.2.2 de R2.

Ejemplo 14.20. Búsqueda de la subred 10.1.2.0/24 y de la subinterfaz S0/0/0.2.

```
R1>show ip interface brief
Interface          IP-Address  OK?   Method   Status                Protocol
FastEthernet0/0    10.1.11.1   YES   NVRAM    up                    up
FastEthernet0/1    unassigned  YES   NVRAM    administratively down down
Serial0/0/0        unassigned  YES   NVRAM    up                    up
Serial0/0/0.2      10.1.2.1    YES   NVRAM    down                  down
Serial0/0/0.5      10.1.5.1    YES   manual   down                  down
Serial0/0/0.34     10.1.34.1   YES   NVRAM    up                    up
R1#show interfaces s 0/0/0.2
Serial0/0/0.2 is down, line protocol is down
  Hardware is GT96K Serial
  Internet address is 10.1.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY
  Last clearing of "show interface" counters never
```

Búsqueda de los PVCs asignados a esa interfaz (Paso 3c)

El comando show frame-relay pvc responde directamente a la cuestión de cuáles son los PVCs que están asignados a qué interfaces y subinterfaces. Si se ejecuta el comando sin parámetros, se muestran aproximadamente diez líneas de resultados para cada VC, y el final de la primera línea contiene la interfaz o subinterfaz asociada. El Ejemplo 14.21 muestra el principio la salida del comando.

Ejemplo 14.21. Correlación de la subinterfaz S0/0/0.2 con el PVC cuyo DLCI es 102.

```
R1>show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

             Active       Inactive     Deleted      Static
 Local         1            2            0           0
 Switched      0            0            0           0
 Unused        0            0            0           0

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE = Serial0/0/0.2

 input pkts 33              output pkts 338        in bytes 1952
 out bytes 29018            dropped pkts 0         in pkts dropped 0
 out pkts dropped 0                 out bytes dropped 0
 in FECN pkts 0             in BECN pkts 0         out FECN pkts 0
 out BECN pkts 0            in DE pkts 0           out DE pkts 0
 out bcast pkts 332         out bcast bytes 28614
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 pvc create time 00:30:05, last time pvc status changed 00:04:14

DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE = Serial0/0/0.34

 input pkts 17              output pkts 24         in bytes 1106
 out bytes 2086             dropped pkts 0         in pkts dropped 0
 out pkts dropped 0                 out bytes dropped 0
 in FECN pkts 0             in BECN pkts 0         out FECN pkts 0
 out BECN pkts 0            in DE pkts 0           out DE pkts 0
 out bcast pkts 11          out bcast bytes 674
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 pvc create time 00:30:07, last time pvc status changed 00:02:57

DLCI = 104, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.34

 input pkts 41              output pkts 42         in bytes 2466
 out bytes 3017             dropped pkts 0         in pkts dropped 0
```

(continúa)

Ejemplo 14.21. Correlación de la subinterfaz S0/0/0.2 con el PVC cuyo DLCI es 102 *(continuación)*.

```
out pkts dropped 0                  out bytes dropped 0
in FECN pkts 0              in BECN pkts 0          out FECN pkts 0
out BECN pkts 0             in DE pkts 0            out DE pkts 0
out bcast pkts 30           out bcast bytes 1929
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:30:07, last time pvc status changed 00:26:17
```

Para buscar todos los PVCs asociados a una interfaz o subinterfaz, basta leer las partes resaltadas del Ejemplo 14.12. En este caso, S0/0/0.2 sólo se muestra en un PVC, el que tiene el DLCI 102, así que en este caso sólo hay un PVC asociado a S0/0/0.2.

Determinación del PVC que se usa para llegar a un determinado vecino (Paso 3d)

Si la configuración del router asocia más de un PVC a una interfaz o subinterfaz, el paso siguiente es determinar cuál de los PVCs se utiliza para enviar tráfico a un determinado vecino. Por ejemplo, el Ejemplo 14.21 muestra que R1 utiliza una subinterfaz multipunto S0/0/0.34 con los DLCIs 103 y 104, empleando el DLCI 103 para el PVC que lleva a R3, y el DLCI 104 para el PVC que se conecta a R4. Por tanto, si estuviéramos resolviendo un problema en el que fallase el comando ping 10.1.34.3 en R1, el paso siguiente consistiría en determinar cuál de los dos DLCIs (103 ó 104) identifica al VC que conecta R1 a R3.

Desafortunadamente, no siempre se puede hallar la respuesta sin examinar otra documentación. El único comando show que puede servir de ayuda es show frame-relay map, que puede correlacionar la dirección IP del siguiente salto con su DLCI. Lamentablemente, si el router local se basa en ARP Inverso, en este momento el router local no puede aprender la información de mapeo, así que la tabla de mapeo quizá no contenga información útil. Sin embargo, si se utiliza un mapeo estático, es posible identificar la combinación correcta de PVC/DLCI.

En el ejemplo en que R1 falla al hacer un ping a 10.1.2.2 (R2) porque sólo hay un PVC asociado a la interfaz correcta (S0/0/0.2), el PVC ya ha sido identificado, así que por el momento se puede ignorar este paso.

Estado de un PVC

En este punto del Paso 3 de la resolución de problemas, ya se ha identificado la interfaz o subinterfaz saliente y la combinación correcta de PVC/DLCI. Finalmente, se puede examinar el estado del PVC para ver si significa que el PVC tiene un problema.

Los routers utilizan cuatro códigos de estado de PVC diferentes. Los routers determinan dos de los posibles valores de estado, *active* e *inactive*, mediante mensajes LMI proce-

dentes del switch Frame Relay. El mensaje LMI del switch enumera los DLCIs de todos los PVCs configurados en ese enlace de acceso, y si el PVC se puede utilizar en ese momento (*active*) o no (*inactive*).

El primero de los dos estados de PVC que no se aprende empleando LMI se denomina estado *static* (estático). Si la LMI está inhabilitada, el router no aprende información alguna relativa al estado del PVC y procedente del switch. Por tanto, el router muestra todos sus DLCIs configurados en el estado *static*, indicando que están configurados estáticamente. El router no sabe si los PVCs funcionarán, pero al menos puede enviar tramas empleando esos DLCIs con la esperanza de que la red Frame Relay pueda entregarlos.

El otro estado de PVC, *deleted*, se utiliza cuando LMI funciona pero los mensajes LMI del switch no mencionan nada sobre un valor concreto de DLCI. Si el router tiene configuración para un DLCI (por ejemplo, en un comando `frame-relay interface-dlci`), pero el mensaje LMI del switch no muestra ese DLCI, entonces el router muestra el DLCI en un estado *deleted*. Este estado significa que el router ha configurado el DLCI pero el switch no. En la vida real, el estado *deleted* puede significar que el router no se ha configurado bien, o que el switch Frame Relay todavía no está configurado con el DLCI correcto. La Tabla 14.4 resume los cuatro códigos de estado de PVC de Frame Relay.

Tabla 14.4. Valores de estado de PVC.

Estado	Active	Inactive	Deleted	Static
El PVC está definido para la red Frame Relay	Sí	Sí	No	Desconocido
El router intentará enviar tramas a través de un VC que se halle en este estado	Sí	No	No	Sí

Según se indica en la última fila de la tabla, los routers sólo pueden enviar datos a través de PVCs que se hallen en un estado activo o estático. Además, aunque el PVC se halle en un estado estático, no hay garantía de que la red Frame Relay pueda realmente enviar tramas a través de ese PVC, porque el estado estático implica que LMI está inhabilitada, y que el router no ha aprendido ninguna información de estado.

El paso siguiente en el proceso de resolución de problemas es determinar el estado del PVC empleado para llegar a un determinado vecino. Prosiguiendo con el problema consistente en que R1 falla al hacer un `ping` a R2 (10.1.2.2), el Ejemplo 14.22 muestra el estado del PVC cuyo DLCI es 102, según se había identificado anteriormente.

En este caso, R1 no puede hacer un `ping` a R2 porque el PVC cuyo DLCI es 102 se halla en estado inactivo.

Para aislar más el problema y determinar la causa principal, es necesario examinar más detalladamente las razones por las que un PVC podría estar en estado inactivo. En primer lugar, como siempre, se repiten los mismos pasos de resolución de problemas en el otro router; en este caso, R2. Si no se hallan problemas en R2, salvo un PVC inactivo, el problema

Ejemplo 14.22. Comando show frame-relay pvc en R1.

```
R1>show frame-relay pvc 102

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE = Serial0/0/0.2

 input pkts 22             output pkts 193          in bytes 1256
 out bytes 16436           dropped pkts 0           in pkts dropped 0
 out pkts dropped 0                 out bytes dropped 0
 in FECN pkts 0            in BECN pkts 0           out FECN pkts 0
 out BECN pkts 0           in DE pkts 0             out DE pkts 0
 out bcast pkts 187        out bcast bytes 16032
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 pvc create time 01:12:56, last time pvc status changed 00:22:45
```

puede ser un problema verdadero en la red del proveedor de Frame Relay, así que el próximo paso puede ser una llamada al proveedor. Sin embargo, quizá aparezca algún otro problema en el router remoto. Por ejemplo, para crear el fallo y los comandos show de esta sección, el enlace de acceso de R2 se desactivó, así que un examen rápido del Paso 1 para la resolución de problemas en el router R2 habría identificado el problema. Sin embargo, si al seguir adelante con el proceso se observa que ambos routers muestran sus extremos del PVC en estado inactivo, la causa principal se halla en la red del proveedor de Frame Relay.

Buscar la causa inicial de un problema relacionado con un PVC en estado *deleted* es relativamente sencillo. Este estado significa que la configuración del switch Frame Relay y la configuración del router no coinciden, y el router se configura con una DLCI que tampoco está configurado en el switch. O bien, el proveedor dijo que iba a configurar un PVC con un determinado DLCI y no lo hizo, o el ingeniero del router lo ha configurado con un valor de DLCI incorrecto.

Estado de la subinterfaz

Las subinterfaces tienen un código de estado de línea y un código de estado de protocolo, exactamente igual que las interfaces físicas. Sin embargo, como las subinterfaces son virtuales, los códigos de estado y sus significados difieren un poquito de las interfaces físicas. Esta sección examina brevemente la forma en que funcionan las subinterfaces de Frame Relay y la forma en que el IOS decide si una subinterfaz de Frame Relay debería estar en un estado *up*/*up* o en un estado *down*/*down*.

La configuración de Frame Relay asocia uno o más DLCIs con una subinterfaz empleando dos comandos: frame-relay interface-dlci y frame-relay map. De todos los DLCIs asociados a una subinterfaz, el IOS utiliza las reglas siguientes para determinar el estado de la misma:

- ***down/down*:** Todos los DLCIs asociados a la subinterfaz están inactivos o borrados, o la interfaz física subyacente no está en el estado *up/up*.
- ***up/up*:** Al menos uno de los DLCIs asociados a la subinterfaz está activo o estático.

Por ejemplo, para causar los problemas mostrados en el Ejemplo 14.22, R2 y R3 se limitan a desactivar sus enlaces de acceso Frame Relay. La Figura 14.8 muestra el próximo mensaje de estado LMI que envía el switch S1 a R1.

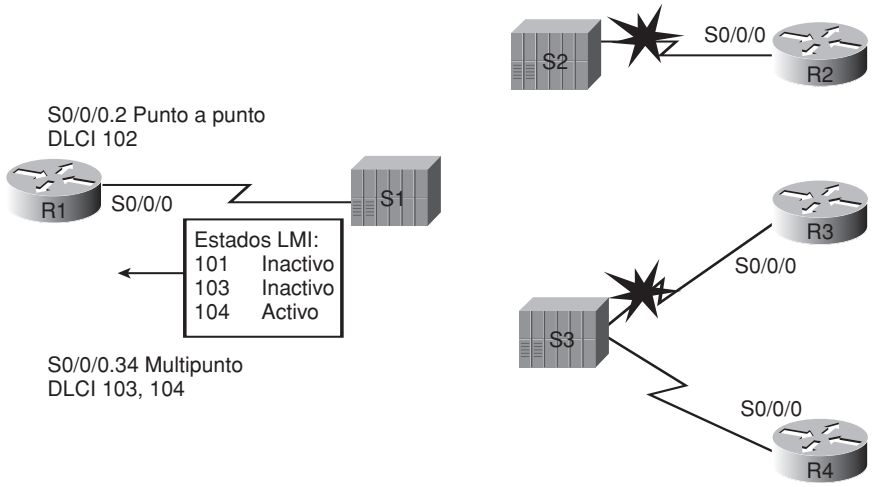


Figura 14.8. Resultados de desactivar los enlaces de acceso en R2 y R3.

Como puede verse en la figura, R1 utiliza una subinterfaz punto a punto (S0/0/0.2) para el VCs que lo conecta a R2, y una subinterfaz multipunto (S0/0/0.34) asociada a los VCs que van a R3 y R4 (103 y 104, respectivamente). El comienzo del Ejemplo 14.20 muestra que S0/0/0.2 se halla en un estado *down/down*, lo cual se debe a que el único DLCI asociado a la subinterfaz (102) está inactivo. Sin embargo, S0/0/0.34 tiene dos DLCIs, uno de los cuales está activo, así que el IOS deja la S0/0/0.34 en un estado *up/up*.

Resulta útil examinar el estado de la subinterfaz cuando se resuelven problemas, pero hay que tener en cuenta que aunque una subinterfaz esté *up*, si se trata de una subinterfaz multipunto, el estado *up/up* no significa necesariamente que todos los DLCIs asociados a la subinterfaz estén operativos.

Problemas de mapeo en Frame Relay (Paso 4)

Si se han seguido los tres primeros pasos del proceso de resolución de problemas sugerido en este capítulo y se han resuelto los problemas que hayan surgido a cada paso, al llegar a este punto las interfaces de enlace de acceso de todos los routers deberían estar en el estado *up/up*, y el PVC que hay entre los dos routers debería hallarse en un estado activo (o está-

tico). Si los routers siguen sin poder hacer un ping a sus respectivas direcciones IP Frame Relay, lo próximo que hay que comprobar es la información relativa al mapeo de direcciones Frame Relay, que asigna los DLCIs a las direcciones IP de siguiente salto.

Esta sección no repite el detallado tratamiento del mapeo de direcciones que aparece tanto en el Capítulo 13 como en este capítulo. Sin embargo, para dar una perspectiva, la lista siguiente pone de manifiesto unos cuantos consejos y pistas que pueden servir como recordatorio cuando se lleva a cabo este paso de resolución de problemas:

En subinterfaces punto a punto:

- Estas subinterfaces no necesitan ARP Inverso ni mapeo estático, porque el IOS piensa simplemente que la subred definida en la subinterfaz es alcanzable a través del único DLCI de la subinterfaz.
- El resultado del comando show frame-relay map sigue mostrando estas subinterfaces, pero sin dirección IP de siguiente salto.

En interfaces físicas y subinterfaces multipunto:

- Tienen que utilizar bien ARP Inverso o mapeo estático.
- El comando show frame-relay map debería mostrar la dirección IP Frame Relay del router remoto y el DLCI del router local para cada PVC asociado a la interfaz o subinterfaz.
- Si se utiliza mapeo estático, se necesita la palabra reservada broadcast para admitir un protocolo de enrutamiento.

Para completar, el Ejemplo 14.23 muestra la salida del comando show frame-relay map en el router R1 de la Figura 14.6, sin problemas con el mapeo. (Los problemas anteriores que se habían introducido ya se han corregido.) En este caso, la interfaz S0/0/0.2 es una subinterfaz punto a punto, y S0/0/0.34 es multipunto, con un mapeo aprendido mediante ARP Inverso y otro mapeo configurado estáticamente.

Ejemplo 14.23. Comando **show frame-relay map** en R1.

```
R1#show frame-relay map
Serial0/0/0.34 (up): ip 10.1.34.4 dlci 104(0x68,0x1880), static,
               broadcast,
               CISCO, status defined, active
Serial0/0/0.34 (up): ip 10.1.34.3 dlci 103(0x67,0x1870), dynamic,
               broadcast,, status defined, active
Serial0/0/0.2 (up): point-to-point dlci, dlci 102(0x66,0x1860), broadcast
          status defined, active
```

Encapsulación entre extremos (Paso 5)

La encapsulación de un extremo a otro en un PVC se refiere a los encabezados que siguen al encabezado de Frame Relay, con dos opciones: el encabezado exclusivo de Cisco y el encabezado estándar del IETF. Los detalles de configuración se han mostrado anteriormente en este capítulo, en la sección "Configuración de la encapsulación y de LMI".

Finalmente, unos ajustes de encapsulación que no coinciden en los routers situados en extremos opuestos del enlace pueden dar lugar a un problema en un caso concreto. Si uno de los routers es de Cisco, y utiliza encapsulación Cisco, y el otro router no es de Cisco, y utiliza encapsulación IETF, entonces pueden fallar los *pings* como consecuencia de la desigualdad de las encapsulaciones. Sin embargo, dos routers de Cisco pueden entender ambos tipos de encapsulación, así que no debería ser problema en redes formadas únicamente por routers de Cisco.

Números de subred desiguales (Paso 6)

En este punto, si los problemas hallados en cinco de los seis primeros pasos de resolución de problemas se han resuelto, todos los problemas de Frame Relay deberían estar solucionados. Sin embargo, si los dos routers que hay en los extremos del PVC han configurado equivocadamente direcciones IP de subredes distintas, entonces los routers no se podrán hacer ping entre sí, y los protocolos de enrutamiento no llegarán a ser adyacentes. Por tanto, como último paso, se deberían confirmar las direcciones IP de cada router, y las máscaras, y habría que asegurarse de que se conectan a la misma subred. Para hacer esto, basta utilizar los comandos show ip interface brief y show interfaces en ambos routers.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetado con un icono en el margen exterior de la página. La Tabla 14.5 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 14.5. Temas clave del Capítulo 14.

Tema clave	Descripción	Número de página
Lista	Lista de comprobación para la configuración de Frame Relay.	493
Lista	Ajustes predeterminados de Frame Relay en el IOS.	495-496
Definición	Concepto y definición de la asignación de direcciones en Frame Relay.	498
Figura 14.3	Proceso de ARP Inverso en Frame Relay.	500
Lista	Lista de comprobación para la resolución de problemas de Frame Relay en seis pasos.	512
Lista	Resumen de las dos funciones principales de la LMI.	514
Tabla 14.4	Lista de valores de estado de PVC y de sus significados.	520
Lista	Razones para que las subinterfaces estén *up*/*up* o *down*/*down*.	522
Lista	Resumen de la información de mapeo que se observa en las subinterfaces punto a punto.	523
Lista	Resumen de la información de mapeo que se observa en las subinterfaces multipunto.	523

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD), o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las

listas. El Apéndice K, "Respuestas a los ejercicios de memorización", que también está disponible en el DVD, incluye las tablas ya completadas para validar su trabajo.

Lectura de los escenarios del Apéndice F

El Apéndice F, "Escenarios adicionales", contiene cinco escenarios detallados que le ofrecen la oportunidad de analizar distintos diseños, problemas y salidas de comandos. También le muestran cómo se interrelacionan los conceptos de varios capítulos diferentes. El Escenario 4 examina toda una gama de opciones y problemas relacionados con la implementación de Frame Relay.

Referencias de comandos

Aunque no necesariamente debe memorizar la información de las tablas de esta sección, ésta incluye una referencia de los comandos de configuración y EXEC utilizados en este capítulo. En la práctica, debería memorizar los comandos como un efecto colateral de leer el capítulo y hacer todas las actividades de esta sección de preparación del examen. Para verificar si ha memorizado los comandos como un efecto colateral de sus otros estudios, cubra el lado izquierdo de la tabla con un pedazo de papel, lea las descripciones del lado derecho y compruebe si recuerda el comando.

Tabla 14.6. Comandos de configuración del Capítulo 14.

Comando	**Descripción**
encapsulation frame-relay [ietf | cisco]	Comando de configuración del modo de interfaz que define la encapsulación Frame Relay que se utiliza en lugar de HDLC, PPP y demás.
frame-relay lmi-type {ansi | q933a | cisco}	Comando de configuración del modo de interfaz que define el tipo de mensajes LMI que se envían al switch.
bandwidth *núm*	Subcomando de interfaz que especifica la velocidad de interfaz que percibe el router.
frame-relay map {*protocolo dirección-protocolo dlci*} [broadcast] [ietf | cisco]	Comando de configuración del modo de interfaz que define estáticamente una asignación entre una dirección de la capa de red y un DLCI.
keepalive *seg*	Comando de configuración del modo de interfaz que define la existencia y periodicidad de mensajes de petición de estado de LMI, tanto a efectos de envío como de recepción.

(continúa)

Tabla 14.6. Comandos de configuración del Capítulo 14 *(continuación).*

Comando	Descripción
interface serial *núm.sub* [point-to-point | multipoint]	Comando del modo de configuración global que crea una subinterfaz o alude a una subinterfaz creada previamente.
frame-relay interface-dlci *dlci* [ietf | cisco]	Comando del modo de configuración de subinterfaz que vincula o relaciona un DLCI con la subinterfaz.

Tabla 14.7. Comandos EXEC del Capítulo 14.

Comando	Descripción
show interfaces [*tipo número*]	Muestra el estado de la interfaz física.
show frame-relay pvc [interface *interfaz*][*dlci*]	Muestra información sobre el estado del PVC.
show frame-relay lmi [*tipo número*]	Muestra información sobre el estado de la LMI.
debug frame-relay lmi	Muestra el contenido de los mensajes LMI.
debug frame-relay events	Muestra los mensajes relativos a ciertos eventos de Frame Relay, incluyendo los mensajes de ARP Inverso.

Este capítulo trata los siguientes temas:

Fundamentos de VPN: Esta sección describe los principales objetivos y beneficios de las VPNs.

VPNs IPsec: Esta sección explica la forma en que la arquitectura del protocolo de Seguridad IP (IPsec) ofrece las características principales que se necesitan tanto en las VPNs entre sedes como en las de acceso.

VPNs SSL: Esta última sección examina el uso del protocolo de Capa de *sockets* seguros (*Secure Socket Layer*, SSL) que se incluye en los navegadores web más comunes actualmente.

CAPÍTULO 15

Redes privadas virtuales

Una compañía que tuviera una sede principal y diez sedes remotas podría comprar diez líneas T1, cada una de las cuales iría de la sede central a cada oficina remota. Una solución más efectiva consistiría en utilizar Frame Relay. Sin embargo, especialmente debido a que las sedes remotas suelen necesitar acceso a Internet es incluso más rentable conectar cada oficina a Internet y enviar el tráfico entre sedes a través de Internet, empleando Internet como una WAN.

Desafortunadamente, la Internet no es en modo alguno tan segura como las líneas alquiladas y Frame Relay. Por ejemplo, para que un atacante robase copias de tramas de datos que pasasen a través de una línea alquilada, tendría que poder acceder físicamente al cable, muy frecuentemente dentro de un edificio seguro, o bajo las calles, o en la oficina central de la empresa de telecomunicaciones; todas estas acciones pueden dar lugar a una sentencia de cárcel. En Internet, un atacante podría buscar formas menos intrusivas de obtener copias de los paquetes, sin siquiera abandonar la computadora de su casa, y con un riesgo mucho menor de dar con sus huesos en la cárcel.

Las redes privadas virtuales (VPN) resuelven el problema de seguridad asociado a utilizar Internet como un servicio WAN. Este capítulo explica los conceptos y terminología de las VPNs.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las seis preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 15.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

1. ¿Cuál de los términos siguientes se refiere a una VPN que utiliza Internet para conectar las sedes de una sola compañía, en lugar de utilizar líneas alquiladas o Frame Relay?

Tabla 15.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
Fundamentos de VPN	1-2
VPNs IPsec	3-5
VPNs SSL	6

a. VPN intranet.

b. VPN extranet.

c. VPN de acceso.

d. VPN empresarial.

2. ¿Cuáles de los siguientes no se consideran objetivos de seguridad deseables para una VPN entre sedes?

a. Comprobaciones de integridad de mensajes.

b. Privacidad (cifrado).

c. Antivirus.

d. Autenticación.

3. ¿Cuáles de las funciones siguientes podrían ser realizadas por el encabezado de autenticación IP de IPsec?

a. Autenticación.

b. Encriptación (cifrado).

c. Comprobaciones de integridad de mensajes.

d. Anti-respuestas.

4. ¿Cuál de los siguientes se considera el mejor protocolo de encriptación para proporcionar privacidad en una VPN IPsec en comparación con las otras respuestas?

a. AES.

b. HMAC-MD5.

c. HMAC-SHA-1.

d. DES.

e. 3DES.

5. ¿Cuál de las tres opciones siguientes serían las opciones de uso más frecuente para componentes VPN de nueva adquisición e instalados en la actualidad?

a. ASA.

b. Cortafuegos PIX.

c. Concentrador VPN.

d. Router de Cisco.

e. Cliente VPN de Cisco.

6. Cuando se utiliza la solución Cisco Web VPN, con el cliente empleando un navegador web normal sin software de cliente especial, ¿cuáles de las afirmaciones siguientes son verdaderas?

a. El usuario crea una conexión TCP a un servidor web VPN empleando SSL.

b. Si el usuario se conecta a un servidor web normal dentro de la empresa, y ese servidor sólo admite HTTP y no SSL, esos paquetes pasan por Internet sin encriptar.

c. El servidor web VPN se conecta a los servidores web internos en nombre del cliente web VPN, traduciendo entre HTTP y SSL cuando sea necesario.

d. El cliente web VPN no se puede conectar sin tener al menos un software SSL de cliente ligero instalado en el cliente.

Temas fundamentales

Este capítulo tiene tres secciones principales. La primera sección presenta el concepto básico de VPN. La segunda sección (y la más extensa) examina algunos de los detalles de la construcción de VPNs empleando las reglas de seguridad que se definen en las RFCs de Seguridad IP (IPsec). La última sección explica las bases de una tecnología de VPN alternativa denominada SSL.

Fundamentos de VPN

Las líneas alquiladas poseen algunas características de seguridad excelentes. El router de un extremo conoce con confianza la identidad del dispositivo que se halla en el otro extremo del enlace. El router receptor también tiene buenas razones para creer que no hay atacantes que hayan visto los datos en tránsito, ni tampoco que hayan modificado los datos para causar algún daño.

Las redes privadas virtuales (VPN) intentan proporcionar las mismas características de seguridad que una línea alquilada. En particular, ofrecen lo siguiente:

- **Privacidad:** Impedir que alguien de Internet (un intermediario) copie el paquete en Internet y pueda leer los datos.
- **Autenticación:** Verificar que el remitente del paquete VPN es un dispositivo legítimo y no un dispositivo empleado por un atacante.
- **Integridad de los datos:** Verificar que el paquete no ha sido modificado mientras transitaba por Internet.

- **Antireproducción:** Impedir que un intermediario copie paquetes enviados por un usuario legítimo, para después volver a enviar los paquetes con objeto de parecer que es un usuario legítimo.

Para llevar a cabo estos propósitos, dos dispositivos próximos al borde de Internet crean una VPN, que a veces se denomina **túnel VPN**. Los dispositivos añaden encabezados al paquete original, y los encabezados contienen campos que permiten a los dispositivos VPN llevar a cabo todas las funciones. Los dispositivos VPN también encriptan el paquete IP original, y esto significa que el contenido original del paquete es indescifrable para alguien que pudiera ver una copia del paquete mientras éste atraviesa Internet.

La Figura 15.1 muestra la idea general de lo que sucede típicamente en un túnel VPN. La figura muestra una VPN creada entre un router de una oficina local y un Dispositivo de seguridad adaptado (ASA) de Cisco. En este caso, la VPN se denomina VPN entre sedes, porque conecta dos sedes de una compañía. Esa VPN también se denomina VPN **intranet** entre sedes, porque conecta sedes que pertenecen a una sola compañía.

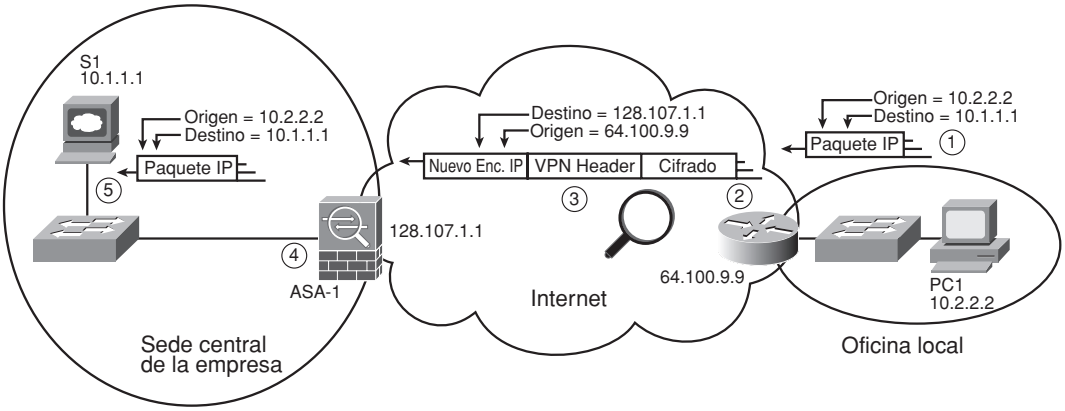


Figura 15.1. Conceptos de túnel VPN para una VPN intranet entre sedes.

La figura muestra los pasos siguientes, que explican el flujo global dentro de la figura:

1. El host PC1 (10.2.2.2) situado en el lado derecho envía un paquete al servidor web (10.1.1.1), tal como lo haría sin una VPN.
2. El router encripta el paquete, añade encabezados VPN, añade otro encabezado IP (con direcciones IP públicas) y reenvía el paquete.
3. Un intermediario copia el paquete pero no puede modificarlo sin ser detectado, y no puede leer el contenido del paquete.
4. ASA-1 recibe el paquete, confirma la autenticidad del remitente, confirma que el paquete no ha sido modificado, y descifra el paquete original.
5. El servidor S1 recibe el paquete descifrado.

Los beneficios de utilizar una VPN basada en Internet como la que se muestra en la Figura 15.1 son muchos. El coste de una conexión de alta velocidad a Internet suele ser mucho

menor que el de una línea alquilada o una WAN Frame Relay. Internet parece estar en todas partes, haciendo que esta clase de solución esté disponible en todo el mundo. Y mediante el uso de protocolos y tecnologías VPN, las comunicaciones resultan ser seguras.

Nota

El término túnel se refiere genéricamente el envío de un paquete de cualquier protocolo que se manda encapsulando el paquete dentro de otro paquete. El término túnel VPN implica que el paquete encapsulado se ha encriptado, mientras que el término túnel no implica si el paquete se ha encriptado o no.

Se pueden construir VPNs empleando toda una gama de dispositivos, y para múltiples propósitos. La Figura 15.2 muestra un ejemplo de tres de las razones primarias que hay para construir una VPN en Internet en la actualidad.

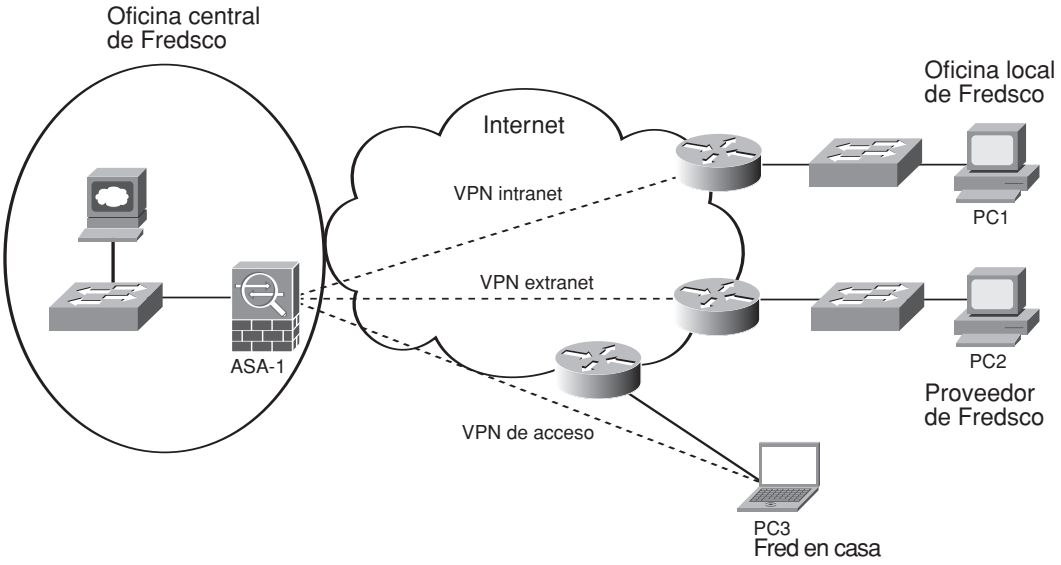


Figura 15.2. VPN intranet, extranet y de acceso.

En la parte superior de la figura, la sede central y una oficina local de una compañía ficticia (Fredsco) están conectadas mediante una VPN intranet. La parte central de la figura muestra a Fredsco conectándose a otra compañía que le suministra piezas, lo cual hace que esa VPN sea una VPN extranet. Por último, cuando Fred se lleva su portátil a casa después de trabajar y se conecta a Internet, la conexión segura a través de VPN desde el portátil hasta la red de Fredsco se denomina VPN de acceso remoto, o simplemente VPN de acceso. En este caso, el portátil en sí es el extremo de un túnel VPN, en lugar del router de acceso a Internet. La Tabla 15.2 resume las características principales de estos tres tipos de VPNs.

Tema clave

Tabla 15.2. Tipos de VPNs.

Tipo	Propósito práctico
Intranet	Conecta todas las computadoras de la misma organización, normalmente empleando un dispositivo VPN en cada sede.
Extranet	Conecta todas las computadoras de dos sedes de organizaciones distintas pero asociadas, normalmente empleando un dispositivo VPN en cada sede.
Acceso	Conecta a usuarios de Internet individuales con la red empresarial.

Para construir una VPN, es necesario que un dispositivo de cada sede posea hardware y/o software que comprenda un conjunto seleccionado de estándares y protocolos de seguridad VPN. Entre estos dispositivos se cuentan los siguientes:

- **Routers:** Además de reenviar paquetes, el router puede ofrecer también funciones de VPN. El router puede tener tarjetas adicionales especializadas que le ayuden a efectuar la encriptación con más rapidez.
- **Dispositivo de seguridad adaptativo (ASA):** Es el dispositivo más conocido de Cisco para la seguridad; se puede configurar para realizar muchas funciones de seguridad, incluyendo las VPNs.
- **Cortafuegos PIX:** Es la línea anterior de cortafuegos de Cisco; pueden realizar funciones de VPN además de operar como cortafuegos. Las nuevas instalaciones actuales utilizarían un ASA.
- **Concentradores VPN:** Es una línea antigua de productos de Cisco; estos dispositivos ofrecen una plataforma hardware que actúa específicamente como el punto final de un túnel VPN. Las nuevas instalaciones actuales utilizarían un ASA.
- **Cliente VPN:** Para las VPNs de acceso, el PC podría tener que realizar funciones de VPN; el portátil necesita un software para realizar esas funciones y ese software se denomina **cliente VPN**.

A continuación, el texto examina el uso de un conjunto de protocolos denominados IPsec para crear VPNs.

VPNs IPsec

IPsec es una arquitectura o conjunto de funcionalidades que ofrece servicios de seguridad para redes. El nombre en sí no es un acrónimo, sino más bien una abreviatura del título de la RFC que lo define (RFC 4301, *Security Architecture for the Internet Protocol*), y que suele denominarse IP Security (Seguridad IP), o IPsec.

IPsec define un conjunto de funciones, por ejemplo para autenticación y encriptación, y algunas reglas relativas a cada una de esas funciones. Sin embargo, al igual que la arquitectura del conjunto de protocolos TCP/IP define muchos protocolos, algunos de los cua-

les son alternativas de otros, IPsec permite utilizar varias opciones distintas de protocolos para cada característica de las VPNs. Una de las ventajas de IPsec es que su papel como arquitectura permite que se le hagan adiciones y modificaciones a lo largo del tiempo, a medida que se hacen mejoras en los protocolos de seguridad.

Las secciones siguientes examinan los componentes de IPsec, comenzando por la encriptación, que va seguida por el intercambio de claves, la integridad de los mensajes y la autenticación.

Encriptación IPsec

Si se ignora el aspecto matemático (y, afortunadamente, esto es posible) entonces la encriptación IPsec no es demasiado difícil de entender. La encriptación de IPsec hace uso de un par de algoritmos de encriptación, que en esencia son fórmulas matemáticas y que satisfacen un par de requisitos. En primer lugar, las dos fórmulas matemáticas forman una pareja:

- Una de ellas oculta (encripta) los datos.
- Otra revela (desencripta) los datos originales a partir de los datos encriptados.

Además de esas funciones más o menos evidentes, las dos fórmulas matemáticas se han seleccionado de tal modo que si se intercepta el texto encriptado, pero no se dispone de la contraseña secreta (que se llama clave de encriptación) entonces va a ser difícil desencriptar ese paquete. Además, las fórmulas se han seleccionado de tal modo que si un atacante consiguiera desencriptar un paquete, la información no le ofrecería ventaja alguna para desencriptar los otros paquetes.

El proceso para encriptar datos para una VPN IPsec funciona generalmente como se muestra en la Figura 15.3. Obsérvese que la clave de encriptación también se conoce como clave de sesión, clave compartida o clave compartida de sesión.

Los cuatro pasos resaltados en la figura son los siguientes:

1. El dispositivo VPN emisor (como el router de la oficina local de la Figura 15.1) inserta el paquete original y la clave de sesión en la fórmula de encriptación, calculando los datos encriptados.
2. El dispositivo emisor encapsula los datos encriptados en un paquete, que incluye el nuevo encabezado IP y el encabezado VPN.
3. El dispositivo emisor envía este nuevo paquete al dispositivo VPN de destino (que es ASA-1 en la Figura 15.1).
4. El dispositivo VPN receptor ejecuta la correspondiente fórmula de desencriptación, empleando los datos encriptados y la clave de sesión (que es el mismo valor que se ha utilizado en el dispositivo VPN emisor) para desencriptar los datos.

IPsec admite ciertas variaciones en los algoritmos de encriptación, algunas de las cuales son simplemente de desarrollo más reciente y mejores, mientras que otras tienen compensaciones. En particular, la longitud de la clave tiene una cierta influencia, aumentando la dificultad para que los atacantes desencripten los datos (las claves más largas hacen el

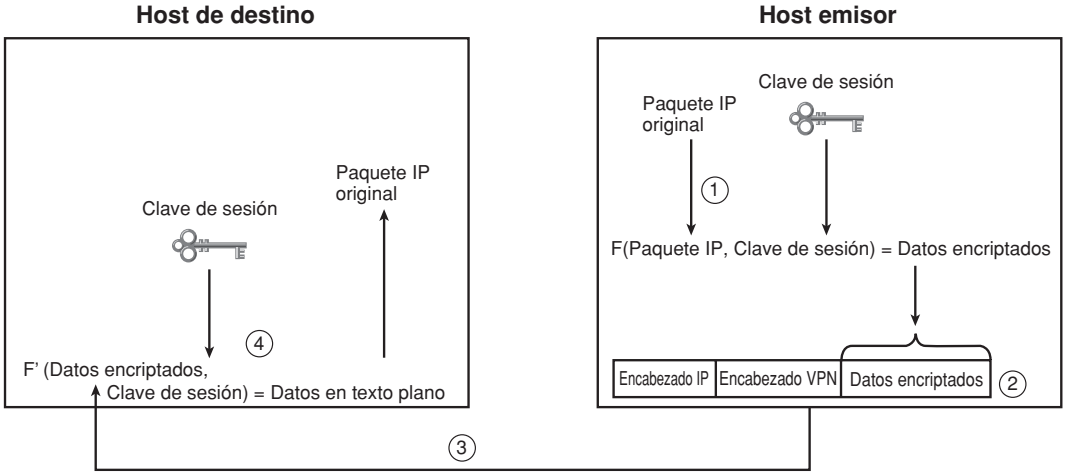


Figura 15.3. Proceso básico de encriptación IPsec.

proceso más difícil), pero con un resultado negativo porque en general se necesita más potencia de procesamiento. La Tabla 15.3 resume varias de estas opciones y las longitudes de las claves.

Tabla 15.3. Comparación de algoritmos de encriptación para VPN.

Algoritmos de encriptación	Longitud de la clave (bits)	Comentarios
Estándar de cifrado de datos (DES)	56	Más antiguo y menos seguro que las otras opciones que se muestran aquí.
Triple DES (3DES)	56 × 3	Aplica tres claves DES de 56 bits en sucesión mejorando la potencia de encriptación respecto a DES.
Estándar avanzado de cifrado (AES)	128 y 256	Se considera el mejor en la actualidad, y ofrece una encriptación fuerte al mismo tiempo que menos exigencias de cálculo que 3DES.

Intercambio de claves en IPsec

El uso de una clave común compartida (que también se denomina clave simétrica) para la encriptación da lugar a un problema similar al del huevo y la gallina: si ambos dispositivos necesitan conocer el mismo valor de la clave antes de que puedan encriptar y desencriptar datos, ¿cómo pueden estos dispositivos enviar los valores de la clave a través de la red sin tener que enviar las claves como texto plano, quedando así expuestos a que robe las claves un atacante?

El problema relacionado con la **distribución de claves** ha existido desde que se creó la encriptación por primera vez. Una opción sencilla pero problemática consiste en utilizar Claves precompartidas (PSK), que es una forma bonita de decir que se configuran manualmente los valores en ambos dispositivos. Si se emplean las PSKs, sería lo mismo llamar por teléfono al ingeniero de la oficinal local, o enviarlas por carta, o (no haga esto en casa) mandarlas por correo electrónico inseguro.

El problema de las PSKs es que aunque nadie llegue a robar la clave de encriptación compartida, la naturaleza humana hará que las PSKs no cambien casi nunca. Es como cambiar la contraseña en un sitio web que nunca exige que se cambie la contraseña: quizá no se nos ocurra nunca, nadie nos obliga y no deseamos tener que recordar una contraseña nueva. Sin embargo, para mejorar la seguridad, es necesario modificar las claves ocasionalmente, porque a pesar de que los algoritmos de encriptación hacen difícil desencriptar los datos, es técnicamente posible para un atacante obtener la clave, y de este modo desencriptar el paquete. Los protocolos con cambio dinámico de claves permiten cambiar frecuentemente las claves de encriptación, y de esta forma se reduce significativamente la cantidad de datos que se pierden si un atacante llega a comprometer una clave de encriptación.

IPsec, como arquitectura de seguridad, requiere usar un **intercambio dinámico de claves** mediante un proceso definido por la RFC 4306 y denominado Intercambio de clave de Internet (*Internet Key Exchange*, IKE). IKE (RFC 4306) requiere utilizar un proceso específico de intercambio de claves llamado intercambio de Diffie-Hellman (DH), cuyo nombre proviene de los inventores del proceso. El intercambio de claves DH supera el problema del huevo y la gallina mediante un algoritmo que permite a los dispositivos crear e intercambiar claves de forma segura, evitando que alguien que pueda ver los mensajes llegue a deducir el valor de la clave.

La opción primaria de configuración para el intercambio de claves DH es la longitud de las claves que utiliza el proceso de intercambio de claves DH para encriptar los mensajes de intercambio de claves. Cuanto más larga sea la clave de encriptación que es preciso intercambiar, más larga tiene que ser la clave DH. La Tabla 15.4 resume las tres opciones principales.

Tabla 15.4. Opciones de DH.

Opción	Longitud de la clave
DH-1	768 bits
DH-2	1024 bits
DH-5	1536 bits

Autenticación e integridad de mensajes en IPsec

IPsec posee también varias opciones para el proceso de autenticación y para mantener la integridad de los mensajes. En general, la autenticación se refiere al proceso mediante el

cual un dispositivo VPN receptor puede confirmar que un paquete ha sido enviado realmente por un igual VPN en que puede confiar. La integridad de los mensajes, que a veces se denomina autenticación de mensajes, permite al receptor confirmar que el mensaje no ha sido modificado en tránsito.

Las comprobaciones de autentificación e integridad de mensajes de IPsec emplean algunos de los conceptos generales propios del proceso de encriptación de intercambio de claves, así que este texto no profundizará demasiado en este asunto. Sin embargo, resulta útil comprender los conceptos básicos.

Las comprobaciones de integridad de los mensajes se pueden realizar mediante el protocolo de Encabezado de autenticación (*Authentication Header*, AH) de IPsec que utiliza un concepto de clave compartida (simétrica) pero empleando una función *hash* (dispersión) en lugar de una función de encriptación. La dispersión opera de forma similar al concepto de secuencia de verificación de trama (*frame check sequence*, FCS) que se aplica en la información final de la mayoría de los protocolos de enlace de datos, pero de una forma mucho más segura. La dispersión (que es un cierto tipo de función matemática), cuyo nombre formal es Código de autenticación de mensajes basado en la dispersión (*Hashed-based Message Authentication Code*, HMAC) da lugar a un número pequeño que se puede almacenar en uno de los encabezados VPN. El emisor calcula la dispersión y envía los resultados en el encabezado VPN. El receptor recalcula la dispersión, empleando la misma clave compartida (el mismo valor de la clave en ambos extremos), y compara el valor calculado con el valor mostrado en el encabezado VPN. Si los valores coinciden, significa que los datos suministrados a la fórmula por el remitente coinciden con los suministrados a la fórmula por el receptor, así que el receptor sabe que el mensaje no se ha visto modificado durante el tránsito.

Estas funciones de comprobación de la integridad con HMAC utilizan normalmente una clave secreta que tiene que ser al menos dos veces más larga que la clave de encriptación con que se ha codificado el mensaje. Como resultado, se han creado varias opciones de HMAC con el paso de los años. Por ejemplo, el estándar basado en el algoritmo de compendio de mensajes 5 (MD5) utiliza una clave de 128 bits, que le permite admitir VPNs que utilicen una longitud de clave de encriptación DES de 56 bits.

Nota

Si la VPN utiliza ESP para encriptar paquetes, no se precisa la función de integridad de mensajes HMAC porque el atacante tendría que superar la clave de encriptación antes de que pudiera alterar el contenido del mensaje.

El proceso de autenticación emplea un concepto de clave pública/privada similar al intercambio de claves DH, y se basa en la idea consistente en que el valor encriptado con la clave privada del emisor se puede desencriptar con la clave pública del emisor. Al igual que en la comprobación de integridad de mensajes, el emisor calcula un valor y lo pone en el encabezado VPN, pero esta vez lo hace empleando la clave privada del emisor. El receptor utiliza la clave pública del emisor para desencriptar el valor transmitido, y lo compara con el valor mostrado en el encabezado. Si coinciden los valores, el receptor sabe que el emisor es auténtico.

La Tabla 15.5 resume algunos de los protocolos y herramientas específicos que se utilizan para la autenticación y comprobación de integridad de mensajes en IPsec.

Tabla 15.5. Opciones de autenticación y de comprobación de integridad de mensajes en IPsec.

Función	Método	Descripción
Integridad del mensaje	HMAC-MD5	HMAC-MD5 utiliza una clave compartida de 128 bits, y genera un valor disperso de 128 bits.
Integridad del mensaje	HMAC-SHA	El algoritmo de dispersión segura HMAC define distintos tamaños de la clave (por ejemplo, SHA-1 [160], SHA-256 [256] y SHA-512 [512]) para admitir distintos tamaños de claves de encriptación. Se considera mejor que MD5 pero se requiere un mayor tiempo de cálculo.
Autenticación	Claves precompartidas	Los dos dispositivos VPN tienen que ser configurados previamente con la misma clave secreta.
Autenticación	Firmas digitales	También reciben el nombre de firmas Rivest, Shamir y Adelman (RSA). El emisor encripta un valor con su clave privada; el receptor desencripta con la clave pública del emisor y lo compara con el valor que ha puesto el emisor en el encabezado.

Protocolos de seguridad ESP y AH

Para desempeñar las funciones de VPN descritas en este capítulo, IPsec define dos protocolos de seguridad, y cada protocolo define un encabezado. Estos encabezados se han mostrado de forma genérica en la Figura 15.1 como encabezados de VPN. Los encabezados tan sólo proporcionan un lugar para almacenar información necesaria para las distintas funciones de VPN. Por ejemplo, el proceso de verificación de la integridad del mensaje requiere que el emisor ubique los resultados de la función *hash* en un encabezado, y que transmita el encabezado (como parte del mensaje completo) al dispositivo VPN receptor, que a su vez utilizará el valor almacenado en ese encabezado para completar la comprobación de integridad del mensaje.

Dos de los protocolos definidos por IPsec son el de Sobrecarga de seguridad del encapsulado (*Encapsulating Security Payload*, ESP) y el de Encabezado de autenticación IP (*IP Authentication Header*, AH). ESP define reglas para llevar a cabo las cuatro misiones fundamentales de las VPNs, según se ha indicado a lo largo de este capítulo y resumido en la Tabla 15.6. AH admite dos posibilidades, a saber, la autenticación y la integridad del mensaje. Una VPN IPsec podría utilizar sólo uno de los dos encabezados, o los dos. Por ejemplo, AH podría proporcionar la autenticación y la integridad de mensajes, y ESP ofrecería la privacidad de los datos (la encriptación).

Tema clave

Tabla 15.6. Resumen de las funciones ofrecidas por ESP y AH.

Característica	¿La posee ESP?	¿La posee AH?
Autenticación	Sí (débil)	Sí (fuerte)
Integridad de los mensajes	Sí	Sí
Encriptación	Sí	No
Anti-reproduccion	Sí	No

Consideraciones sobre la implementación de IPsec

Las VPNs IPsec ofrecen una conexión segura a través de la Internet insegura, de tal modo que las computadoras se pueden comportar como si estuviesen conectadas directamente a la red corporativa. Para las VPNs entre sedes, las computadoras de usuario final ni siquiera saben que existe una VPN, tal como sucedería con una línea alquilada o una WAN basada en Frame Relay. El usuario puede emplear cualquier aplicación, exactamente igual que si estuviera conectado a la LAN en la oficina principal.

Los usuarios de una VPN de acceso remoto con IPsec disfrutan de las mismas funciones que los usuarios de VPN entre sedes, y pueden acceder a todas y cada una de las aplicaciones permitidas. Sin embargo, las VPNs de acceso remoto requieren un cierto esfuerzo adicional, porque cada computadora necesita utilizar el software de cliente VPN de Cisco. Este software implementa los estándares IPsec en el PC, en lugar de requerir un soporte de VPN en un dispositivo adicional. La instalación no es difícil, pero supone un poquito más de trabajo por cada computadora, mientras que en comparación con una VPN entre sedes implementada con un router de Cisco ya instalado, el único requisito podría ser una actualización del IOS de Cisco.

Para facilitar la instalación y configuración de VPNs, Cisco ofrece un entorno y un conjunto de funciones llamado **Easy VPN**. El problema que resuelve Easy VPN se puede comprender fácilmente considerando el ejemplo siguiente. Una compañía tiene 200 sitios remotos con los que quiere crear una VPN intranet empleando Internet. Además, esta compañía quiere tener conexiones VPN extranet entre sedes con una docena de asociados. Por último, 2000 empleados tienen sus propios portátiles, y todos ellos (al menos ocasionalmente) se llevan a casa los portátiles y se conectan a la red de la empresa a través de Internet. IPsec tiene muchas opciones para cada función, y requiere efectuar una configuración en cada sitio.

Easy VPN ayuda a resolver los problemas administrativos en un entorno similar al descrito, permitiendo que un servidor Cisco Easy VPN, que normalmente será el dispositivo VPN de la sede central, comunique dinámicamente a los dispositivos de sitios remotos sus configuraciones VPN IPsec. Los dispositivos remotos (routers, ASA, portátiles con el software de

cliente VPN de Cisco y demás) actúan como clientes Easy VPN, conectándose al servidor Easy VPN y descargando los ajustes de configuración.

A continuación, la sección final de este capítulo examina brevemente una tecnología VPN alternativa que se denomina SSL.

VPNs SSL

Los navegadores web de uso frecuente en la actualidad admiten un protocolo denominado ***Secure Socket Layer (SSL)***. Estos navegadores suelen admitir también otro estándar posterior pero menos conocido y denominado Seguridad de la capa de transporte *(Transport Layer Security, TLS)*. Esta sección explica la forma en que se puede utilizar SSL para crear VPNs de acceso.

Nota

En lugar de aludir tanto a SSL como a TLS a lo largo de toda la sección, el texto utiliza únicamente el término SSL, que es de uso más frecuente. SSL y TLS no son protocolos realmente equivalentes, pero desempeñan las mismas funciones y son iguales hasta el nivel de profundidad que se describe en este capítulo.

Los navegadores web utilizan HTTP para conectarse a los servidores web. Sin embargo, cuando es necesario que las comunicaciones con el servidor web sean seguras, el navegador pasa a utilizar SSL. SSL utiliza el puerto conocido 443, y encripta los datos enviados entre el navegador y el servidor, además de autenticar al usuario. Después, los mensajes HTTP fluyen a través de la conexión SSL.

Casi todo el mundo ha utilizado alguna vez SSL, y muchas veces sin saberlo. Si alguna vez ha visitado un sitio web de Internet y necesitaba proporcionar información relativa a una tarjeta de crédito o alguna otra información personal, es probable que el navegador haya pasado a utilizar SSL. Casi todos los navegadores muestran un icono que se parece a un candado, con el candado abierto cuando no se utiliza SSL y cerrado cuando se usa SSL.

Los navegadores web pueden decidir cuándo y cómo van a implementar SSL. Como SSL requiere más trabajo, muchos servidores web utilizan sólo HTTP para proporcionar información general, y pasan a SSL sólo cuando el usuario tiene que aportar información personal, como las credenciales de conexión e información financiera. Sin embargo, cuando los servidores web internos de una empresa necesitan enviar datos a un usuario doméstico situado al otro lado de Internet, y no a un usuario de la LAN local de la empresa, es posible que el servidor necesite hacer seguras todas las comunicaciones con el cliente para evitar pérdidas de datos.

Cisco resuelve algunos de los problemas asociados al acceso web interno para usuarios basados en Internet mediante una posibilidad llamada Web VPN. A diferencia de las VPNs IPsec, Web VPN típicamente sólo admite tráfico web, y no todo tipo de tráfico. Sin embargo, una inmensa mayoría de las aplicaciones empresariales actuales están habilitadas para la Web. Por ejemplo, casi todos los usuarios finales necesitan accede a aplicaciones inter-

nas, que se ejecutan desde servidores web internos y posiblemente también necesiten acceder a un servidor de correo electrónico. Si un usuario puede comprobar el correo electrónico desde un navegador web, entonces la mayoría de las funciones que necesita ese usuario se pueden efectuar desde un navegador web, si no son todas, y Web VPN puede ofrecer una solución razonable.

Web VPN asegura la conexión de un usuario doméstico con la red de su empresa mediante el uso de SSL entre el usuario final y un servidor Web VPN especial. La Figura 15.4 muestra una visión general.

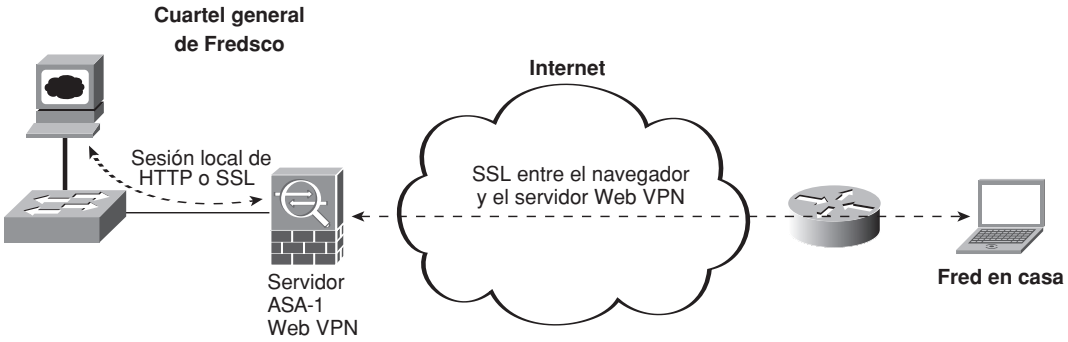


Figura 15.4. Web VPN Using SSL

Para utilizar Web VPN, el usuario basado en Internet abre cualquier navegador web y se conecta a un servidor Web VPN Cisco. El servidor VPN se puede implementar en muchos dispositivos, incluyendo un ASA. Esta conexión utiliza SSL para todas las comunicaciones, empleando las capacidades de SSL que tiene el navegador web, de tal modo que todas las comunicaciones entre el cliente y el servidor web son seguras.

El servidor Web VPN se comporta como servidor web y presenta una página web al cliente. La página web muestra las aplicaciones de la empresa que están disponibles para el cliente. Por ejemplo, puede mostrar todas las aplicaciones basadas en la Web que son típicas de una empresa, el servidor de correo electrónico basado en la Web y otros servicios basados en la Web. Cuando el usuario selecciona una opción, el servidor Web VPN se conecta a ese servicio, empleando HTTP o SSL, según lo requiera el servidor. Entonces el servidor Web VPN pasa el tráfico HTTP/SSL desde y hacia el servidor real a través de la conexión SSL y llega hasta el cliente basado en Internet. Como resultado, todas las comunicaciones que pasan por Internet se aseguran mediante SSL.

La ventaja de esta solución basada en Web VPN consiste en que no requiere ni un software ni un esfuerzo especial por parte del cliente. Los empleados pueden hasta utilizar su computadora doméstica, la computadora de otra persona o cualquier computadora conectada a Internet, y conectar con el nombre de host del servidor Web VPN.

El aspecto negativo de Web VPN es que sólo permite utilizar un navegador web. Si se necesita utilizar una aplicación a la que no sea posible acceder empleando un navegador,

se dispone de dos opciones. En primer lugar, se podría implementar una VPN IPsec, como ya se ha descrito. Alternativamente, se podría utilizar una variante de Web VPN en que la computadora cliente carga un cliente ligero basado en SSL, empleando un concepto muy similar al del cliente VPN basado en IPsec de Cisco que se emplea en VPN IPsec. Entonces la computadora cliente podría conectarse al servidor Web VPN empleando el cliente ligero, y el servidor Web VPN se limitaría a pasar el tráfico del PC a través de la LAN local, permitiéndole acceder como si el cliente estuviera conectado a la red principal de la empresa.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 15.7 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 15.7. Temas clave del Capítulo 15.

Tema clave	Descripción	Número de página
Lista	Características de seguridad deseadas para las VPNs.	531-532
Tabla 15.2	Tres tipos de VPNs y sus propósitos típicos.	534
Figura 15.3	Partes significativas del proceso de encriptación de VPN.	536
Tabla 15.3	Detalles de los tres algoritmos de encriptación de VPN IPsec para encriptar todo el paquete.	536
Tabla 15.4	Tres opciones de intercambio de clave DH y de longitudes de clave.	537
Tabla 15.6	Resumen de las funciones que admiten los protocolos IPsec ESP y AH.	540

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD) o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo, y compruebe sus respuestas en el glosario:

Clave compartida, cliente VPN, Intercambio de claves Diffie-Hellman, IPsec, SSL, VPN, Web VPN

Temas del examen* ICND2 publicados por Cisco que se tratan en esta parte

Implementar un esquema de direccionamiento IP y de servicios IP destinado a satisfacer los requisitos de red en la red de una oficina local de una empresa de tamaño medio

- Describir los requisitos técnicos para emplear IPv6 (incluyendo protocolos, pila dual, túneles, etc.).
- Describir las direcciones de IPv6.

Implementar, verificar y resolver problemas de NAT y ACL en la red de la oficina local de una empresa de tamaño medio.

- Explicar el funcionamiento básico de NAT.
- Configurar la Conversión de direcciones de red para los requisitos de red dados empleando la CLI.
- Resolución de los problemas de implementación de NAT.

* No olvide consultar en http://www.cisco.com los últimos temas de examen publicados.

PARTE V

Escalado del espacio de direcciones IP

Capítulo 16 Conversión de direcciones de red

Capítulo 17 IP Versión 6

Este capítulo trata los siguientes temas:

Perspectivas sobre la escalabilidad de direcciones en IPv4: Esta sección explica la necesidad más significativa que dio lugar al desarrollo de NAT en la década de los 90.

Conceptos de conversión de direcciones de red: Esta sección explica la forma en que operan distintas variantes de NAT.

Configuración y resolución de problemas en NAT: Esta sección describe la forma de configurar NAT, así como la manera de utilizar comandos `show` y `debug` para resolver problemas de NAT.

CAPÍTULO 16

Conversión de direcciones de red

Este capítulo marca el comienzo de la Parte V, "Escalado del espacio de direcciones IP". Los dos capítulos de esta parte del libro están relacionados entre sí porque explican las dos soluciones más importantes de lo que fuera un enorme obstáculo para el crecimiento de Internet. El problema era que el espacio de direcciones de IPv4 se habría consumido en su totalidad a mediados de la década de los 90 si no se hubieran aportado unas soluciones significativas. Una de las soluciones más importantes a corto plazo fue la Conversión de direcciones de red (*Network Address Translation*, NAT), que es el foco de este capítulo. La solución más significativa a largo plazo es IPv6, que ataca el problema haciendo que el espacio de direcciones sea extremadamente grande. IPv6 se tratará en el capítulo siguiente.

Este capítulo comienza con un breve tratamiento del Enrutamiento entre dominios sin clase (*Classless Interdomain Routing*, CIDR), que ayuda a los proveedores de servicios de Internet (ISP) a gestionar el espacio de direcciones IP, y del direccionamiento IP privado. La mayor parte del resto del capítulo explica los conceptos y configuraciones relacionados con NAT.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las nueve preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 16.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

1. ¿Qué significa CIDR?

- **a.** Classful IP Default Routing.
- **b.** Classful IP D-class Routing.
- **c.** Classful Interdomain Routing.

Tabla 16.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
Perspectivas de la escalabilidad de direcciones en IPv4	1-3
Conceptos de conversión de direcciones de red	4-5
Configuración y resolución de problemas en NAT	6-9

d. Classless IP Default Routing.

e. Classless IP D-class Routing.

f. Classless Interdomain Routing.

2. ¿Cuáles de las siguientes subredes resumidas que representan rutas se podrían haber creado para el objetivo de CIDR consistente en reducir el tamaño de las tablas de enrutamiento de Internet?

a. 10.0.0.0 255.255.255.0

b. 10.1.0.0 255.255.0.0

c. 200.1.1.0 255.255.255.0

d. 200.1.0.0 255.255.0.0

3. ¿Cuáles de las siguientes no son direcciones privadas según la RFC 1918?

a. 172.31.1.1

b. 172.33.1.1

c. 10.255.1.1

d. 10.1.255.1

e. 191.168.1.1

4. Empleando NAT estática y efectuando solamente la conversión para direcciones internas, ¿qué da lugar a que se creen entradas en la tabla de NAT?

a. El primer paquete que va desde la red interna hasta la externa.

b. El primer paquete que va desde la red externa hasta la interna.

c. Cuando se configura utilizando el comando ip nat inside source.

d. Cuando se configura utilizando el comando ip nat outside source.

5. Empleando NAT dinámica y efectuando solamente la conversión para direcciones internas, ¿qué da lugar a que se creen entradas en la tabla NAT?

a. El primer paquete que va desde la red interna hasta la externa.

b. El primer paquete que va desde la red externa hasta la interna.

c. Cuando se configura utilizando el comando ip nat inside source.

d. Cuando se configura utilizando el comando ip nat outside source.

6. NAT se ha configurado para traducir las direcciones de origen de los paquetes que se reciben desde dentro de la red, pero sólo para ciertos hosts. ¿Cuál de los comandos siguientes identifica a esos hosts?
   a. ip nat inside source list 1 pool barney
   b. ip nat pool barney 200.1.1.1 200.1.1.254 netmask 255.255.255.0
   c. ip nat inside
   d. ip nat inside 200.1.1.1 200.1.1.2
   e. Ninguna de las otras respuestas es correcta.
7. NAT se ha configurado para traducir las direcciones de origen de los paquetes que se reciben desde dentro de la red, pero sólo para ciertos hosts. ¿Cuál de los siguientes comandos identifica las direcciones IP locales externas que se convierten?
   a. ip nat inside source list 1 pool barney
   b. ip nat pool barney 200.1.1.1 200.1.1.254 netmask 255.255.255.0
   c. ip nat inside
   d. ip nat inside 200.1.1.1 200.1.1.2
   e. Ninguna de las otras respuestas es correcta.
8. Examine los siguientes comandos de configuración:

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
interface Serial0/0
 ip address 200.1.1.249 255.255.255.252
ip nat inside source list 1 interface Serial0/0
access-list 1 permit 10.1.1.0 0.0.0.255
```

   Si la configuración está destinada a habilitar la sobrecarga de NAT en origen, ¿cuál de los comandos siguientes podría ser útil para completar la configuración?
   a. El comando ip nat outside
   b. El comando ip nat pat
   c. La palabra reservada overload
   d. El comando ip nat pool
9. Examine la salida del siguiente comando show en un router configurado para ofrecer NAT dinámica:

```
-- Inside Source
access-list 1 pool fred refcount 2288
 pool fred: netmask 255.255.255.240
    start 200.1.1.1 end 200.1.1.7
    type generic, total addresses 7, allocated 7 (100%), misses 965
```

   Los usuarios se quejan de que no consiguen llegar a Internet. ¿Cuál de las siguientes es la causa más probable?
   a. El problema no está relacionado con NAT, tomando como base la información que ofrece la salida del comando.

b. El almacén NAT no dispone de entradas suficientes para satisfacer todas las solicitudes.

c. No se puede utilizar el estándar ACL 1; es preciso utilizar una ACL extendida.

d. La salida del comando no proporciona información suficiente para identificar el problema.

Temas fundamentales

Este capítulo trata los detalles de NAT, en tres secciones principales. La primera sección explica las dificultades planteadas al espacio de direcciones IPv4 por la revolución de Internet de la década de los 90. La segunda sección explica el concepto básico que subyace a NAT, la forma en que operan algunas variantes de NAT, y la forma en que se conserva el espacio de direcciones IPv4 empleando la Conversión de direcciones de puerto (*Port Address Translation*, PAT). La última sección muestra la forma de configurar NAT mediante el software IOS de Cisco, empleando la interfaz de línea de comandos (CLI) y la forma de resolver problemas de NAT.

Para aquellos que sigan el plan de lectura opcional consistente en ir y venir entre este libro y el libro **CCENT/CCNA ICND1**, obsérvese que el Capítulo 17 de ese libro también trata NAT y PAT, siendo efectuada la configuración desde el Administrador de seguridad de dispositivo (*Security Device Manager*, SDM). Este capítulo trata necesariamente los mismos conceptos subyacentes, pero con una descripción mucho más completa de los conceptos y de la configuración.

Perspectivas sobre la escalabilidad de direcciones en IPv4

El diseño original de Internet requería que todas las organizaciones solicitasen y recibiesen uno o más números de red IP con clase registrados. Quienes administraban el programa se aseguraban de que no se reutilizase ninguna de las direcciones IP. Mientras toda organización utilizase únicamente direcciones IP pertenecientes a sus propios números de red registrados, las direcciones IP nunca serían duplicadas, y el erutamiento IP podía funcionar bien.

La conexión a Internet empleando únicamente un número de red registrado, o varios números de red registrados, funcionó bien durante algún tiempo. A principios de la década de los 90, quedó claro que Internet crecía tan deprisa que todos los números de red IP se habrían reservado a mediados de la década. Se temía que las redes disponibles quedasen completamente reservadas y que algunas organizaciones no pudieran conectarse a Internet.

La solución principal a largo plazo para el problema de la escalabilidad de direcciones IP consistía en incrementar el tamaño de la dirección IP. Este hecho concreto era la razón más convincente para el advenimiento de IP versión 6 (IPv6). (La versión 5 se había definido mucho antes, pero nunca llegó a implantarse, así que el intento siguiente recibió el nombre de versión 6.) IPv6 utiliza una dirección de 128 bits, en lugar de la dirección de 32 bits utilizada en IPv4. Manteniendo o mejorando el proceso de asignación de rangos exclusivos de direcciones a todas las organizaciones conectadas a Internet, IPv6 puede admitir fácilmente a todas las organizaciones e individuos del planeta, puesto que el número de direcciones IPv6 puede superar teóricamente la cifra 10^{38}.

Se sugirieron muchas soluciones a corto plazo para el problema del direccionamiento, pero hubo tres estándares que cooperaron para resolver el problema. Dos de los estándares colaboran estrechamente: Conversión de direcciones de red (NAT) y el direccionamiento privado. Estos mecanismos, en su conjunto, permiten a las organizaciones utilizar internamente números IP no registrados, y comunicarse perfectamente con Internet. El tercer estándar, Enrutamiento entre dominios sin clase (CIDR), permite a los ISPs reducir el desperdicio de direcciones IP asignando a una compañía un subconjunto de un número de red, en lugar de asignarle toda la red. CIDR también puede permitir a los ISPs resumir rutas de tal modo que múltiples redes de clase A, B o C estén asociadas a una sola ruta, lo cual ayuda a reducir el tamaño de las tablas de enrutamiento de Internet.

CIDR

CIDR es una convención global para la asignación de direcciones, que define la forma en que la *Internet Assigned Numbers Authority* (IANA), sus agencias miembros y los ISPs deben asignar direcciones IPv4 globalmente exclusivas a organizaciones individuales. CIDR, que está definido en la RFC 4632 (http://www.ietf.org/rfc/rfc4632.txt), tiene dos objetivos principales. En primer lugar, su política implica que las opciones de asignación de direcciones debe servir de ayuda en el proceso de agregar (resumir) múltiples números de red en una sola entidad de enrutamiento, reduciendo así el tamaño de las tablas de enrutamiento de los routers de Internet. El segundo objetivo es permitir que los ISPs asignen rangos de direcciones a sus clientes, en lugar de una red de clase A, B o C entera, reduciendo de este modo el desaprovechamiento y alejando el momento en que ya no queden más direcciones IPv4 disponibles para asignárselas a nuevas organizaciones y a personas que deseen conectarse a Internet. Las secciones siguientes explican algunos detalles más de los dos objetivos principales de CIDR.

Agregación de rutas para lograr tablas de enrutamiento más breves

Uno de los objetivos principales de CIRD es permitir una agregación de rutas más sencilla en Internet. Imagínese un router de Internet que tuviera una ruta para todas y cada una de las redes de clase A, B y C del planeta. ¡Hay más de dos millones de redes de clase C! Si los routers de Internet tuvieran que enumerar todas las redes con clase en sus tablas

de enrutamiento, los routers necesitarían muchísima memoria y las búsquedas en las tablas de enrutamiento requerirían mucha potencia de cálculo. Al agregar las rutas, se necesitaría que existiesen menos rutas en la tabla de enrutamiento.

La Figura 16.1 muestra un caso típico de la forma en que se podría emplear CIDR para consolidar múltiples redes de clase C en una sola ruta. En esta figura, imagine que el ISP 1 posee las redes de clase C de la 198.0.0.0 a la 198.255.255.0 (pueden parecer curiosos, pero son números válidos de red de clase C). Sin CIDR, todas las tablas de enrutamiento de los otros ISPs tendrían una ruta distinta para cada una de las 2^{16} redes de clase C que empiezan por 198. Con CIDR, como se muestra en la figura, los routers de los otros ISPs tienen una sola ruta que va hasta la 198.0.0.0/8; en otras palabras, una ruta para todos los hosts cuya dirección IP comienza por 198. Hay más de 2 millones de redes de clase C, pero CIDR ha ayudado a los routers de Internet a reducir sus tablas de enrutamiento a un tamaño más manejable. A principios de 2007, las tablas de Internet contenían poco más de 200.000 rutas.

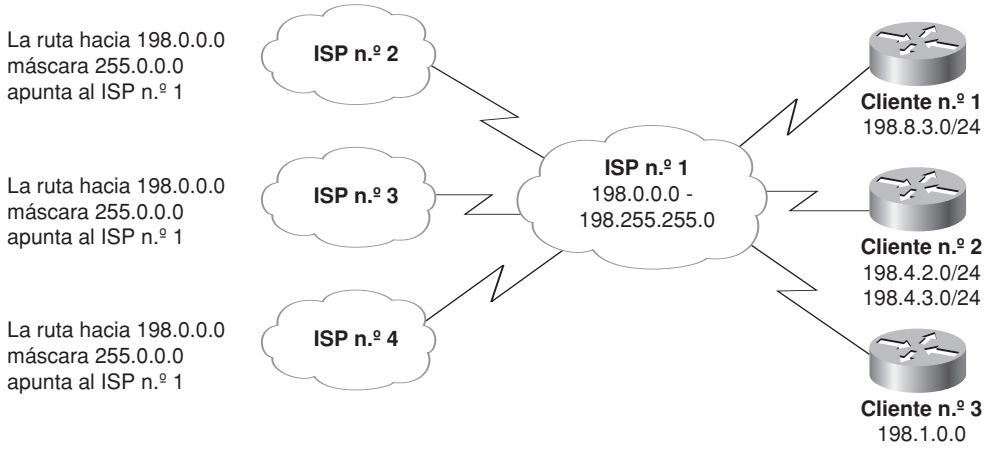


Figura 16.1. Aplicación típica de CIDR.

Al utilizar un protocolo de enrutamiento que intercambia la máscara, así como el número de red o subred, se puede conseguir una visión del número **sin clase**. En otras palabras, se trata el agrupamiento como un problema matemático, ignorando las reglas de las clases A, B y C. Por ejemplo, 198.0.0.0/8 (198.0.0.0, con máscara 255.0.0.0) define un conjunto de direcciones cuyos ocho primeros bits tienen el valor decimal 198. El ISP 1 publica esta ruta a los demás ISPs, que sólo necesitan una ruta para acceder a 198.0.0.0/8. En sus routers, el ISP 1 sabe qué redes de clase C se encuentran en las sedes de qué clientes. Así es como CIDR da a los routers de Internet una tabla de enrutamiento mucho más escalable, reduciendo el número de entradas que hay en las tablas.

Para que CIDR opere tal como se muestra en la Figura 16.1, los ISPs necesitan controlar números de red consecutivos. En la actualidad, las redes IP son asignadas por autoridades

administrativas de distintas regiones del mundo. Las regiones, a su vez, asignan intervalos consecutivos de números de red a ISPs concretos de esas regiones. Esto permite resumir múltiples redes en una sola ruta, como se muestra en la Figura 16.1.

Conservación de direcciones IPv4

CIDR también ayuda a reducir la posibilidad de quedarse sin direcciones IPv4 para nuevas compañías que se conecten a Internet. Además, CIDR permite a los ISPs asignar un subconjunto de una red de clase A, B o C a un determinado cliente. Por ejemplo, imagine que el cliente 1 del ISP 1 necesita sólo diez direcciones IP, y que el cliente 3 necesita 25 direcciones IP. Entonces el ISP 1 hace algo parecido a lo siguiente: asigna la subred IP 198.8.3.16/28, que tiene las direcciones asignables que van de 198.8.3.17 a 198.8.3.30, al cliente 1. Para el cliente 3, el ISP 1 sugiere 198.8.3.32/27, con 30 direcciones asignables (de 198.8.3.33 a 198.8.3.62). El ISP ha satisfecho las necesidades del cliente y no ha tenido que utilizar todas las redes de clase C 198.8.3.0.

CIDR ayuda a impedir el desperdicio de direcciones IP, reduciendo de este modo la necesidad de números de red IP registrados. En lugar de tener dos clientes que consumen dos redes completas de clase C, cada uno consume una pequeña parte de de una sola red de clase C. Además, CIDR, junto con una administración inteligente de los números de red consecutivos por parte de cada ISP, permite que la tabla de enrutamiento de Internet admita una tabla de enrutamiento mucho más pequeña en los routers de Internet que la que sería necesaria de no hacerlo así.

Direccionamiento privado

Ciertas computadoras quizá no lleguen nunca a conectarse a Internet. Las direcciones IP de estas computadoras podrían ser duplicados de direcciones IP de Internet. Cuando se diseña la convención de direccionamiento IP para una red como ésta, una organización puede seleccionar y utilizar cualquier número o colección de números de red que desee, y todo irá bien. Por ejemplo, se pueden comprar unos cuantos routers, se conectan en la oficina y se configuran direcciones IP de la red 1.0.0.0, y todo va bien. Las direcciones IP utilizadas podrían ser duplicados de direcciones IP reales de Internet, pero si lo único que se desea es aprender en el laboratorio, se pueden utilizar números de red denominados **internets privadas**, según lo definido en la RFC 1918, *Address Allocation for Private Internets* (http://www.ietf.org/rfc/rfc1918.txt). Esta RFC define un conjunto de redes que nunca serán asignadas a ninguna organización como número de red registrado. En lugar de utilizar los números de red registrados de alguna otra empresa, se pueden utilizar números de un rango que no va a ser utilizado por nadie más dentro de la Internet pública. La Tabla 16.2 muestra el espacio de direcciones privadas que ha sido definido en la RFC 1918.

En otras palabras, cualquier organización puede emplear estos números de red. Sin embargo, no se permite que ninguna organización publique estas redes empleando un protocolo de enrutamiento en Internet.

Tema clave

Tabla 16.2. Espacio de direcciones privadas definido en la RFC 1918.

Rango de direcciones IP	Clases de redes	Número de redes
10.0.0.0 .0 a 10.255.255.255	A	1
172.16.0.0 .0 a 172.31.255.255	B	16
192.168.0.0 .0 a 192.168.255.255	C	256

Quizá se pregunte por qué va uno a molestarse en reservar números especiales para redes privadas cuando realmente no importa si esas direcciones son duplicados o no. A decir verdad, lo que ocurre es que se puede utilizar un direccionamiento privado en una red interna, y conectarse a Internet al mismo tiempo, siempre y cuando se utilice el mecanismo de Conversión de direcciones de red (NAT). El resto del capítulo está dedicado a examinar y explicar el funcionamiento de NAT.

Conceptos de conversión de direcciones de red

NAT, que está definida en la RFC 3022, permite a un host que no tiene una dirección IP globalmente exclusiva, registrada y válida comunicarse con otros hosts a través de Internet. Los hosts pueden estar utilizando direcciones privadas o direcciones asignadas a otra organización. En ambos casos, NAT permite seguir utilizando estas direcciones que no están preparadas para Internet y sigue permitiendo las comunicaciones con otros hosts a través de Internet.

NAT consigue este objetivo empleando una dirección IP válida registrada para representar la dirección privada frente al resto de Internet. La funcionalidad de NAT cambia las direcciones IP privadas por direcciones IP registradas públicamente dentro de cada paquete, según se muestra en la Figura 16.2.

Obsérvese que el router, que efectúa la NAT, cambia la dirección IP de origen del paquete cuando ese paquete abandona la organización privada. El router que lleva a cabo la NAT modifica también la dirección de destino de todos los paquetes que se reenvían dentro de la red privada. (La red 200.1.1.0 de la Figura 16.2 es una red registrada.) La funcionalidad de NAT, que se ha configurado en el router rotulado como NAT, efectúa la conversión.

El software IOS de Cisco admite varias variantes de NAT. En las próximas páginas se tratan los conceptos que subyacen a algunas de estas variantes. La sección siguiente trata la configuración asociada a cada opción.

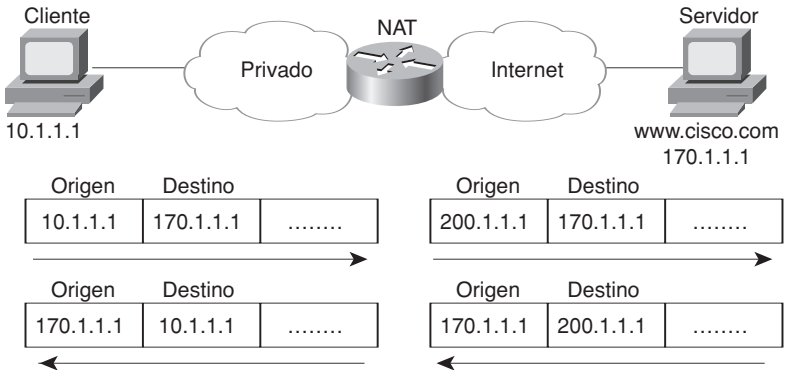


Figura 16.2. Intercambio de direcciones IP mediante NAT: direccionamiento privado.

NAT estática

La NAT estática funciona exactamente igual que el ejemplo mostrado en la Figura 16.2, pero con direcciones IP asignadas estáticamente entre sí. Para ayudarle a comprender las implicaciones de la NAT estática, y para explicar varios términos clave, la Figura 16.3 muestra un ejemplo similar pero con más información.

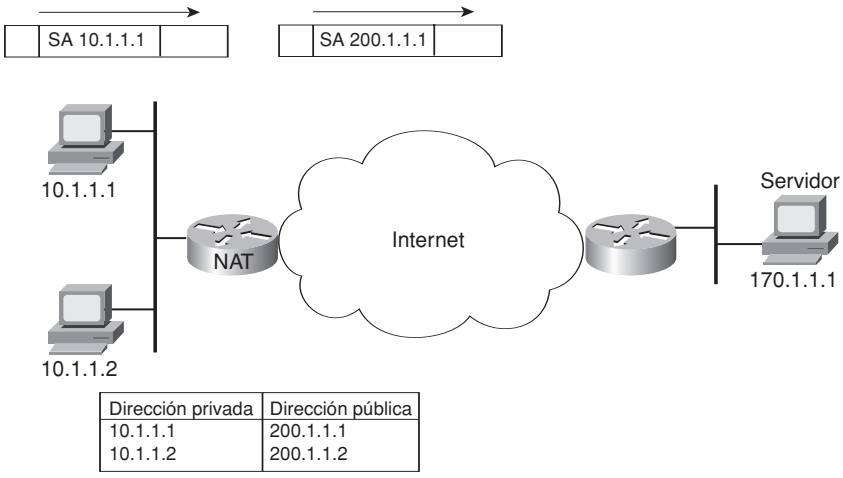


Figura 16.3. NAT estática, mostrando las direcciones locales internas y las direcciones globales.

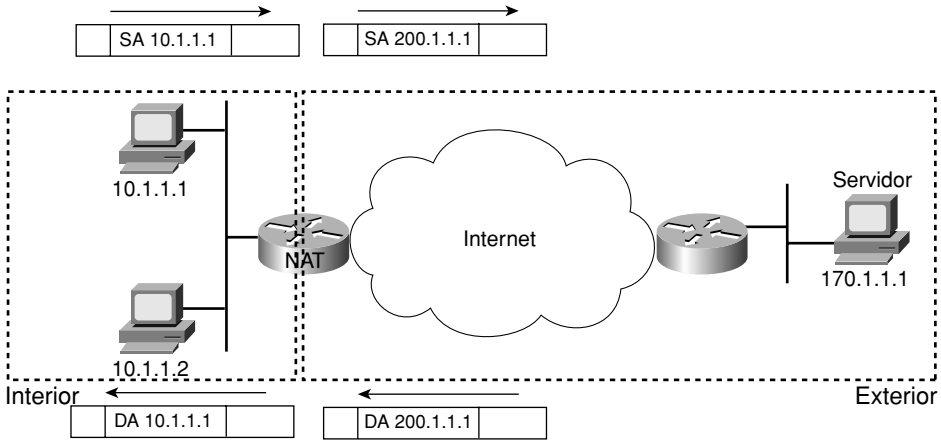
En primer lugar, los conceptos: el ISP de la compañía le ha asignado la red registrada 200.1.1.0. Por tanto, el router NAT tiene que hacer que las direcciones IP privadas parezcan estar en la red 200.1.1.0. Para lograr esto, el router NAT cambia las direcciones IP de origen que hay en los paquetes que van de izquierda a derecha en la figura.

En este ejemplo, el router NAT modifica la dirección de origen ("SA" en la figura) de 10.1.1.1 a 200.1.1.1. Al emplear NAT estática, el router NAT se limita a configurar una asignación de "uno a uno" entre la dirección privada y la dirección registrada que se utiliza en su nombre. El router NAT ha configurado estáticamente una asignación entre la dirección privada 10.1.1.1 y la dirección pública y registrada 200.1.1.1.

Para admitir dos hosts IP en la red privada se necesita una segunda asignación de "uno a uno" estática, empleando una segunda dirección IP del rango público. Por ejemplo, para soportar la dirección 10.1.1.2, el router asigna estáticamente 10.1.1.2 a 200.1.1.2. Como la empresa tiene una sola red registrada de clase C, puede admitir como máximo 254 direcciones IP privadas mediante NAT, con los dos números habituales reservados (el número de red y la dirección de difusión de red).

La terminología que se utiliza en NAT, especialmente en la configuración, puede resultar un poquito confusa. Obsérvese en la Figura 13.6 que la tabla de NAT enumera las direcciones IP privadas como "privadas" y las direcciones públicas y registradas de la red 200.1.1.0 como "públicas". Cisco utiliza el término **local interna** para las direcciones IP privadas de este ejemplo, y el término **global interna** para las direcciones IP públicas.

En la terminología de Cisco, la red empresarial que utiliza direcciones privadas, y por tanto necesita NAT, es la parte "interna" de la red. El lado de Internet de la funcionalidad de NAT es la parte "externa" de la red. El host que precisa NAT (como 10.1.1.1 en el ejemplo) tiene la dirección IP que utiliza dentro de la red, y necesita una dirección IP que lo representa en al red externa. Por tanto, dado que el host necesita esencialmente dos direcciones diferentes para representarlo, se necesitan dos términos. Cisco llama a la dirección IP privada que se utiliza en la red interna la dirección **local interna** y a la dirección que se utiliza para representar al host en el resto de Internet la dirección **global interna**. La Figura 16.4 repite el mismo ejemplo, mostrando parte de la terminología.



Local interna	Global interna
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Figura 16.4. Terminología de NAT estática.

La mayoría de las configuraciones típicas de NAT modifican únicamente la dirección IP de los hosts internos. Por tanto, la tabla NAT actual que se muestra en la Figura 16.4 muestra las direcciones locales internas y las correspondientes direcciones registradas globales internas. Sin embargo, las direcciones IP de hosts externos también se pueden modificar mediante NAT. Cuando esto sucede, los términos **local externa** y **global externa** denotan la dirección IP que se emplea para representar a ese host en las redes interna y externa, respectivamente. La Tabla 16.3 resume la terminología y sus significados.

Tabla 16.3. Términos de direccionamiento en NAT

Tema clave

Término	Significado
Local interna	En un diseño típico de NAT, el término **interno** denota una dirección que se utiliza para un host situado dentro de una empresa. Una dirección local interna es la dirección IP realmente asignada a un host de la red empresarial privada. Se podría utilizar un término más descriptivo, como **interna privada**.
Global interna	En un diseño típico de NAT, el término **interno** denota una dirección que se utiliza para un host situado dentro de una empresa. NAT utiliza las direcciones globales internas para representar el host interno cuando el paquete se envía a través de la red externa, normalmente a través de Internet. El router NAT cambia la dirección IP original de los paquetes que se envían desde una dirección local interna dándole como valor una dirección global interna cuando el paquete va desde la red interna a la externa. Se podría utilizar un término más descriptivo, como **pública interna**, porque cuando se utilizan direcciones de la RFC 1918 en una empresa, la dirección global interna representa al host interno mediante una dirección IP pública que se puede emplear para el enrutamiento en la Internet pública.
Global externa	En un diseño típico de NAT, el término **externo** se refiere a una dirección que se emplea para un host situado fuera de una empresa, en otras palabras, para un host situado en Internet. La dirección global externa es la dirección IP real que se le asigna a un host que reside en la red externa, que típicamente es Internet. Se podría utilizar un término más descriptivo, como **pública externa**, porque la dirección global externa representa al host externo mediante una dirección IP pública que se puede emplear para el enrutamiento en la Internet pública.
Local externa	NAT puede traducir la dirección IP externa (la dirección IP que representa al host fuera de la red empresarial) aunque ésta no es una opción de uso frecuente. Cuando un router NAT reenvía un paquete desde la red interna hasta la externa, y se utiliza NAT para la dirección externa, la dirección IP que representa al host externo como dirección IP de destino en el encabezado del paquete se denomina dirección IP local externa. Se podría utilizar un término más descriptivo, como **privada externa**, porque cuando se utilizan direcciones de la RFC 1918 en una empresa, la dirección local externa representa al host externo mediante una dirección IP privada de la RFC 1918.

NAT dinámica

La NAT dinámica posee ciertas analogías y diferencias con la NAT dinámica. Al igual que la NAT estática, el router NAT crea una asignación "de uno a uno" entre una dirección local interna y una dirección global interna, y cambia las direcciones IP de los paquetes cuando salen y entran en la red interna. Sin embargo, el mapeo de una dirección local interna a una dirección global interna se produce dinámicamente.

La NAT dinámica establece un almacén de direcciones globales internas posibles, y define los criterios correspondientes para determinar qué direcciones IP locales internas deberían convertirse mediante NAT. Por ejemplo, en la Figura 16.5, se ha establecido un almacén formado por cinco direcciones IP globales internas: desde 200.1.1.1 hasta 200.1.1.5. Además se ha configurado NAT para que convierta todas las direcciones locales internas que comiencen por 10.1.1.

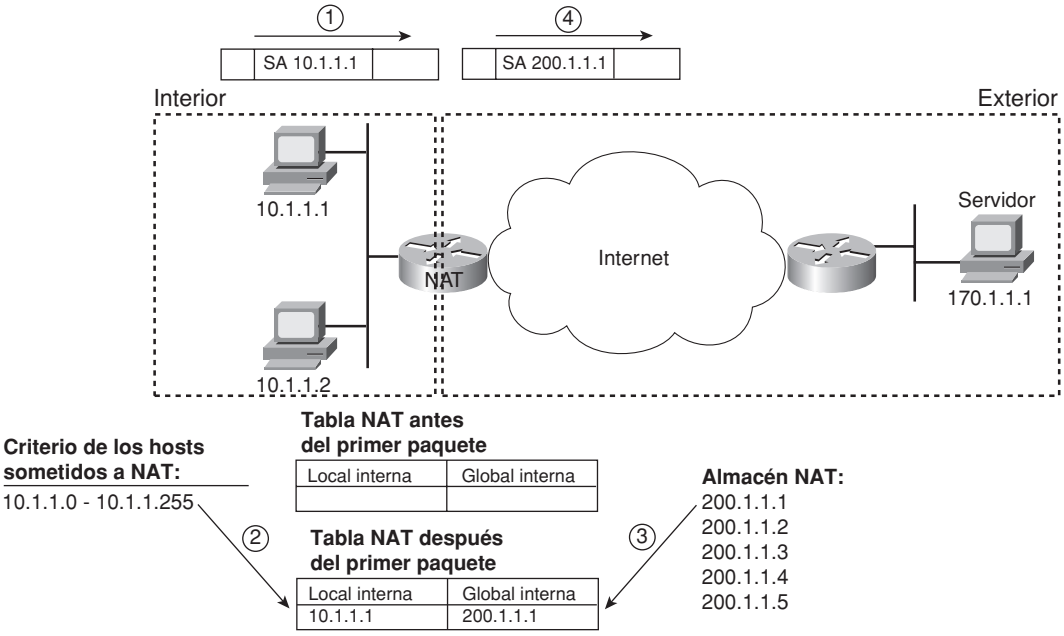


Figura 16.5. NAT dinámica.

Los números 1, 2, 3 y 4 de la figura se refieren a la siguiente sucesión de eventos:

1. El elemento 10.1.1.1 envía su primer paquete al servidor ubicado en 170.1.1.1.
2. Cuando el paquete entra en el router NAT, el router aplica la lógica de búsqueda para decidir si el paquete debe experimentar una NAT. Como la lógica se ha configurado de tal modo que admita las direcciones IP que comienzan por 10.1.1, el router añade una entrada en la tabla NAT para 10.1.1.1 como una dirección local interna.

3. El router NAT necesita asignar una dirección IP del almacén de direcciones globales internas válidas. Selecciona la primera que está disponible (200.1.1.1, en este caso) y la añade a la tabla NAT para completar la entrada.
4. El router NAT traduce la dirección IP original y reenvía el paquete.

La entrada dinámica permanece en la tabla mientras haya un tráfico que fluya ocasionalmente. Se puede configurar una duración máxima que define el tiempo que debe esperar el router, sin haber traducido ningún paquete con esa dirección, antes de descartar la entrada dinámica. También se pueden borrar manualmente las entradas de la tabla empleando el comando `clear ip nat translation*`.

NAT se puede configurar con más direcciones IP en la lista de direcciones locales internas que en el almacén de direcciones globales internas. El router va asignando direcciones del almacén hasta que todas están reservadas. Si llega un paquete nuevo desde algún otro host interno, y necesita una entrada NAT, pero se están utilizando ya todas las direcciones IP del almacén, entonces el router se limita a descartar el paquete. El usuario debe intentarlo de nuevo hasta que alguna entrada NAT supere el tiempo máximo, momento en el cual la función de NAT será operativa para el próximo host que envíe un paquete. En esencia, el almacén de direcciones globales internas tiene que ser de igual tamaño que el número máximo de hosts concurrentes que necesiten utilizar Internet al mismo tiempo, salvo que se utilice PAT, según se explica en la sección siguiente.

Sobrecarga de NAT con la Conversión de direcciones de puerto (*Port Address Translation*, PAT)

Ciertas redes necesitan que la mayoría de sus hosts IP, si no todos, accedan a Internet. Si esa red utiliza direcciones IP privadas, entonces el router NAT requiere un conjunto muy grande de direcciones IP registradas. Si se utiliza NAT estática, para cada host IP privado que necesite acceso a Internet, se necesita una dirección IP registrada públicamente, lo cual se opone frontalmente a nuestro objetivo de reducir el número de direcciones IPv4 públicas que se necesitan para esa organización. La NAT dinámica reduce el problema hasta cierto punto, porque es raro que todos y cada uno de los hosts de una red precisen acceder a Internet simultáneamente. Sin embargo, si un elevado porcentaje de los hosts IP de una red va a necesitar acceder a Internet a lo largo de todo el horario comercial de la compañía, entonces NAT sigue precisando un gran número de direcciones IP registradas, y una vez más no se consigue reducir el consumo de direcciones IPv4.

La función de sobrecargar la NAT, que también se denomina Conversión de direcciones de puerto (PAT), resuelve este problema. La sobrecarga permite a NAT escalar el soporte para muchos clientes con solo unas pocas direcciones IP públicas. La clave para entender el funcionamiento de la sobrecarga consiste en recordar la forma en que los hosts de la red utilizan los puertos TCP y UDP (Protocolo de datagrama de usuario, *User Datagram Protocol*). La Figura 16.6 muestra detalladamente un ejemplo que sirve para que la lógica que subyace a la sobrecarga resulte más evidente.

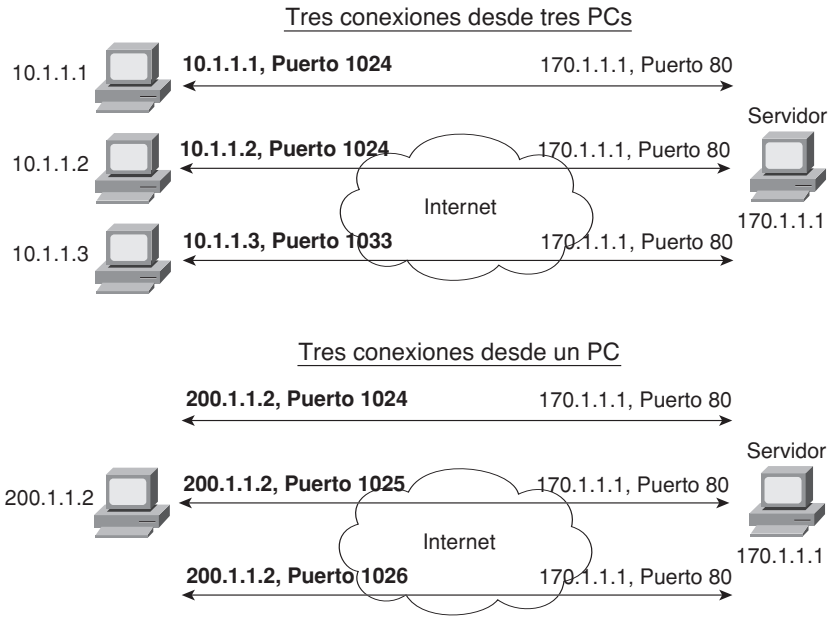


Figura 16.6. Tres conexiones TCP: desde tres hosts distintos y desde uno solo.

La parte superior de la figura muestra una red con tres hosts distintos que se conectan a un servidor web empleando TCP. La parte inferior de la figura muestra la misma red en un momento posterior del día, con tres conexiones TCP de un mismo cliente. Las seis conexiones se conectan a la dirección IP del servidor (170.1.1.1) y al mismo puerto (el 80, que es el puerto conocido para servicios web). En todos los casos, el servidor distingue entre las distintas conexiones porque la combinación de dirección IP y número de puerto es única.

NAT aprovecha el hecho consistente en que al servidor no le importa si tiene una conexión a tres hosts distintos o tres conexiones a una sola dirección IP de host. Por tanto, para admitir muchas direcciones IP locales internas con solo unas pocas direcciones IP registradas que sean globales e internas, la sobrecarga de NAT (PAT) convierte tanto las direcciones como posiblemente también los números de puerto. La Figura 16.7 ilustra la lógica.

Cuando PAT crea la asignación dinámica, selecciona no sólo una dirección IP global interna, sino también un número de puerto exclusivo, que se utilizará con esa dirección. El router NAT mantiene una entrada en la tabla NAT para cada combinación exclusiva de dirección IP local interna y número de puerto, efectuando una conversión a la dirección global interna y un número exclusivo de puerto asociados a la dirección global interna. Y como el campo de número de puerto tiene 16 bits, la sobrecarga de NAT puede utilizar más de 65000 números de puerto, lo cual le permite crecer sin necesitar muchas direcciones IP registradas; en muchos casos, sólo se necesita una dirección IP global externa.

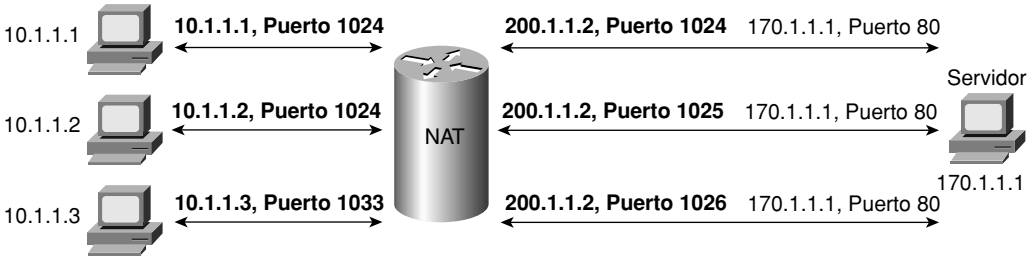


Tabla NAT dinámica con sobrecarga

Local interna	Global interna
10.1.1.1:1024	200.1.1.2:1024
10.1.1.2:1024	200.1.1.2:1025
10.1.1.3:1033	200.1.1.2:1026

Figura 16.7. Sobrecarga de NAT (PAT).

De los tres tipos de NAT descritos en este capítulo, PAT es, con mucho, la opción más popular. Tanto NAT estática como NAT dinámica requieren una asignación "de uno a uno" entre la dirección local interna y la dirección global interna. PAT reduce significativamente el número requerido de direcciones IP registradas en comparación con estas otras alternativas de NAT.

Conversión de direcciones superpuestas

Las tres primeras opciones de NAT explicadas en las secciones anteriores son las que se van a utilizar con mayor probabilidad en la mayoría de las redes. Sin embargo, existe otra variante más de NAT, una que permite convertir tanto la dirección IP de origen como la de destino. Esta opción resulta de especial utilidad cuando dos redes utilizan rangos superpuestos de direcciones IP, por ejemplo cuando una organización no utiliza direccionamiento privado sino que en su lugar emplea un número de red registrado a nombre de otra compañía. Si una compañía utiliza erróneamente un número de red que ha sido correctamente registrado para otra compañía diferente, y ambas se conectan a Internet, se puede utilizar NAT para permitir a ambas compañías comunicarse con hosts situados en Internet y para que se comuniquen entre sí. Para hacer esto, NAT convierte tanto la dirección IP de origen como la de destino. Por ejemplo, considere la Figura 16.8, en la cual una compañía A utiliza una red que está registrada para Cisco (170.1.0.0).

Cuando se tiene un espacio de direcciones superpuestas, un cliente de la compañía A no puede enviar paquetes host cuya IP legítima es 170.1.1.1; si lo hiciera, el paquete nunca llegaría al verdadero 170.1.1.1. ¿Por qué? Las tablas de enrutamiento situadas dentro de la compañía (a la izquierda) posiblemente tengan una ruta que coincida con 170.1.1.1 en su tabla de enrutamiento. Para host 170.1.1.10 de la figura, se encuentra en la subred en que residiría el "privado" 170.1.1.1, así que el host 170.1.1.1 ni siquiera intentaría reenviar los

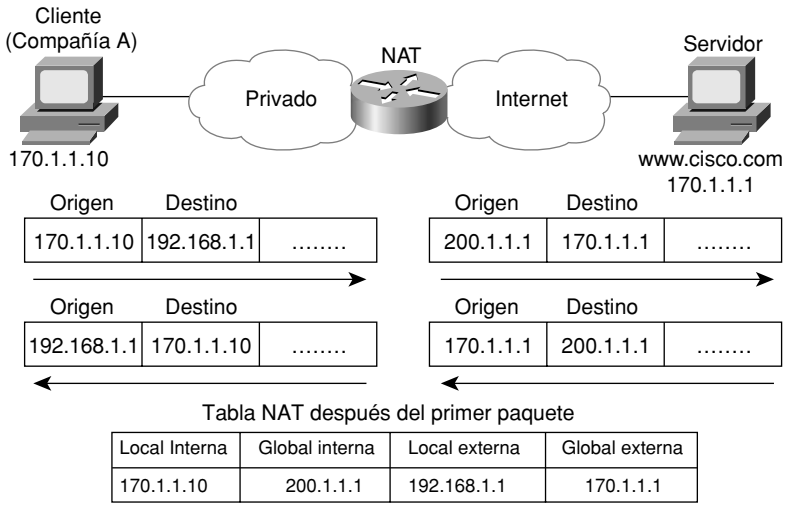


Tabla NAT después del primer paquete

Local Interna	Global interna	Local externa	Global externa
170.1.1.10	200.1.1.1	192.168.1.1	170.1.1.1

Figura 16.8. Intercambio de direcciones IP NAT: redes sin registrar.

paquetes destinados a 170.1.1.1 a un router. En lugar de hacer esto, ¡los reenviaría directamente al host 170.1.1.1, suponiendo que estuviese en la misma LAN! NAT puede resolver este problema, pero tanto la dirección de origen como la de destino tienen que ser modificadas cuando pasa el paquete por el router NAT. En la Figura 16.8, obsérvese que el paquete original enviado por el cliente tiene la dirección de destino 192.168.1.1. Esa dirección, que se llama dirección **local externa**, representa al servidor que se halla fuera de la compañía. *Externa* denota que la dirección representa al host que está ubicado físicamente en la parte "externa" de la red. *Local* significa que esta dirección representa al host que se encuentra en el lado privado de la red.

Cuando el paquete pasa por el router NAT (de izquierda a derecha), la dirección de origen se modifica, igual que en los ejemplos anteriores. Sin embargo, la dirección de destino también se cambia; en este caso pasa a ser 170.1.1.1. La dirección de destino también se denomina dirección **global externa** en este momento, porque representa a un host que siempre se encuentra físicamente en la red externa, y la dirección es la dirección IP global y públicamente registrada que se puede alcanzar a través de Internet.

La configuración de NAT incluye una asignación estática entre la dirección IP real (global externa), 170.1.1.1, y la dirección IP privada (local externa) que se utiliza para representarla dentro de la red privada: 192.168.1.1.

Como el cliente inicia una conexión con el servidor de la derecha, el router NAT no sólo debe traducir direcciones, sino que también debe modificar las respuestas del Sistema de denominación de dominio (*Domain Name System*, DNS). El cliente, por ejemplo, efectúa una solicitud de DNS correspondiente a www.cisco.com. Cuando vuelve la respuesta de DNS (de derecha a izquierda), pasando por el router NAT, NAT cambia la respuesta de DNS de tal manera que el cliente situado en la compañía piensa que la dirección IP de www.cisco.com es192.168.1.1.

En la actualidad, si se vieran obligadas a elegir, las compañías tienden a utilizar el direccionamiento privado para evitar la necesidad de traducir ambas direcciones IP en todos los paquetes. Además, el router NAT precisa una entrada estática para cada servidor que haya en el número de red superpuesto; esto puede ser una tarea muy costosa. Al utilizar direcciones privadas, se puede emplear NAT para conectar la red a la Internet y reducir el número de direcciones IP registradas necesarias, y sólo será preciso aplicar la función NAT a la dirección privada de cada paquete.

La Tabla 16.4 resume el uso de la terminología NAT en la Figura 16.8.

Tabla 16.4. Términos de direccionamiento NAT según se usan en la Figura 16.8.

Término	**Valor de la Figura 16.8**
Local interna	170.1.1.10
Global interna	200.1.1.1
Global externa	170.1.1.1
Local externa	192.168.1.1

Configuración y resolución de problemas en NAT

En las secciones siguientes se ofrece información relativa a la forma de configurar las tres variantes más comunes de NAT: NAT estática, NAT dinámica y PAT, junto con los comandos show y debug que se emplean para la resolución de problemas en NAT.

Configuración de NAT estática

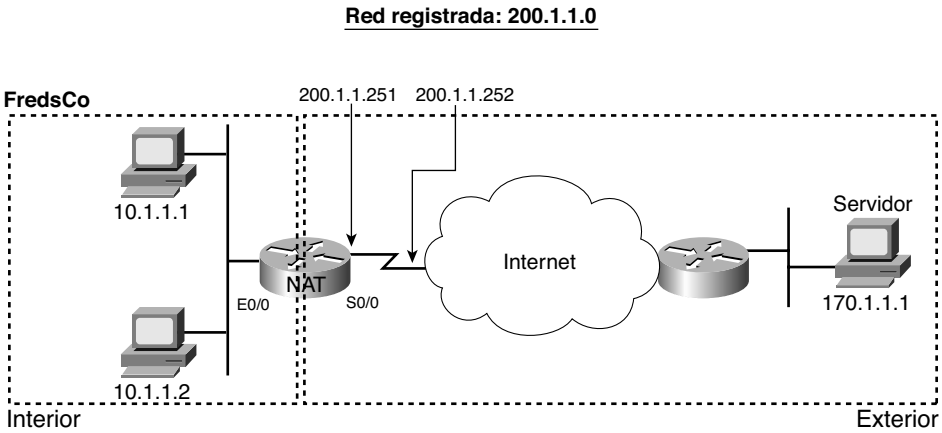
La configuración de NAT estática, en comparación con las demás variantes de NAT, es la que requiere un menor número de pasos de configuración. La asignación estática entre una dirección local (privada) y una dirección global (pública) tiene que ser configurada. Adicionalmente, el router tiene que ser notificado en lo tocante a las interfaces en las que debe utilizar NAT, porque NAT no tiene por qué estar habilitada en todas las interfaces. En particular, el router necesita conocer todas las interfaces y si la interfaz es externa o interna. Los pasos específicos son los siguientes:

Paso 1 Configurar las interfaces que van a estar en la parte interna del diseño de NAT empleando el subcomando de interfaz ip nat inside.

Paso 2 Configurar las interfaces que van a estar en la parte exterior del diseño de NAT empleando el subcomando de interfaz ip nat outside.

Paso 3 Configurar las asignaciones estáticas mediante el comando de configuración global ip nat inside source static *local-interna global-interna*.

La Figura 16.9 muestra la red ya familiar que se ha utilizado en la descripción de NAT estática anteriormente en este capítulo, y que también se ha utilizado para los primeros ejemplos de configuración. En la Figura 16.9 se puede apreciar que FredsCo ha obtenido la red de clase C 200.1.1.0 como número de red registrado. Toda esa red, cuya máscara es 255.255.255.0, está configurada en el enlace serie que media entre FredsCo y la Internet. Al utilizar un enlace serie punto a punto, sólo se consumen dos de las 254 direcciones IP válidas de esa red, y quedan 252 direcciones.



Local interna	Global interna
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Figura 16.9. Intercambio de direcciones IP NAT: redes privadas.

Cuando se planifica una configuración NAT, es preciso hallar ciertas direcciones IP que se usarán como direcciones IP globales internas. Como estas direcciones tienen que formar parte de algún rango de direcciones IP registradas, es frecuente utilizar las direcciones adicionales que hay en la subred que conecta la empresa a Internet; por ejemplo, las 252 direcciones IP adicionales de la red 200.1.1.0 en este caso. El router también se puede configurar con una interfaz *loopback* y se le puede asignar una dirección IP que forme parte de un rango globalmente único de direcciones IP registradas.

El Ejemplo 16.1 muestra la configuración de NAT, empleando 200.1.1.1 y 200.1.1.2 para las dos asignaciones NAT estáticas.

Los mapeos estáticos se crean empleando el comando ip nat inside source static. La palabra reservada inside significa que NAT convierte las direcciones correspondientes a los hosts situados en la parte interna de la red. La palabra reservada source significa que NAT convierte las direcciones IP de origen de los paquetes que llegan a sus interfaces internas. La pala-

Ejemplo 16.1. Configuración de NAT estática.

```
NAT# show running-config
!
! Se han omitido ciertas líneas por brevedad
!
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip nat inside
!
interface Serial0/0
 ip address 200.1.1.251 255.255.255.0
 ip nat outside
!
ip nat inside source static 10.1.1.2 200.1.1.2
ip nat inside source static 10.1.1.1 200.1.1.1

NAT# show ip nat translations
Pro   Inside global    Inside local   Outside local   Outside global
---   200.1.1.1        10.1.1.1       ---             ---
---   200.1.1.2        10.1.1.2       ---             ---

NAT# show ip nat statistics
Total active translations: 2 (2 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/0
Inside interfaces:
  Ethernet0/0
Hits: 100 Misses: 0
Expired translations: 0
Dynamic mappings:
```

bra reservada static significa que los parámetros definen una entrada estática, que nunca debería eliminarse de la tabla NAT por haber superado su duración. Como el diseño requiere que dos hosts, 10.1.1.1 y 10.1.1.2, tengan acceso a Internet, se necesitan dos comandos ip nat inside.

Una vez creadas las entradas NAT estáticas, el router necesita saber qué interfaces son "internas" y cuáles son "externas". Los subcomandos de interfaz ip nat inside e ip nat outside identifican adecuadamente a cada interfaz.

Hay un par de comandos show que muestran la información más importante respecto a NAT. El comando show ip nat translations muestra las dos entradas NAT estáticas que se han creado en la configuración. El comando show ip nat statistics muestra una estadística, indicando cosas tales como el número de entradas que están activas actualmente en la tabla de conversión. La estadística incluye también el número de aciertos, que se incrementa cada vez que llega un paquete para el que NAT tiene que traducir direcciones.

Configuración de NAT dinámica

Como habrá imaginado, la configuración de NAT dinámica se diferencia en algunos aspectos de la NAT estática, pero también tiene algunas similitudes. La NAT dinámica también requiere que se identifiquen todas las interfaces como internas o externas, y por supuesto el mapeo estático ya no se necesita. La NAT dinámica utiliza una lista de control de acceso (ACL) para identificar las direcciones IP locales internas (privadas) que necesitan una traducción de sus direcciones, y define un almacén de direcciones IP públicas registradas que después serán asignadas. Los pasos concretos son como sigue:

Paso 1 Al igual que en la NAT estática, se configuran las interfaces que deben estar en la parte interna del diseño de NAT empleando el subcomando de interfaz ip nat inside.

Paso 2 Al igual que en la NAT estática, se configuran las interfaces que deben estar en la parte externa del diseño de NAT empleando el subcomando de interfaz ip nat outside.

Paso 3 Se configura una ACL que especifica los paquetes que llegan a interfaces internas a los cuales es preciso aplicar NAT.

Paso 4 Se configura el almacén de direcciones IP registradas públicas empleando el comando de configuración global ip nat pool *nombre primera-dirección última-dirección* mask *máscara-de-subred*.

Paso 5 Se habilita la NAT dinámica haciendo referencia a la ACL (Paso 3) y al almacén (Paso 4) en el comando de configuración global ip nat source list *número-acl* pool *nombre-almacén*.

El ejemplo siguiente utiliza la misma topología de red que en el ejemplo anterior (véase la Figura 16.9). En este caso, las dos mismas direcciones locales internas, 10.1.1.1 y 10.1.1.2, necesitan conversión. Las mismas direcciones globales internas empleadas en los mapeos estáticos del ejemplo anterior, 200.1.1.1 y 200.1.1.2, se ponen ahora en un almacén de direcciones globales internas asignables dinámicamente. El Ejemplo 16.2 muestra la configuración y también algunos comandos show.

La configuración de NAT dinámica incluye un almacén de direcciones globales internas, así como una lista de acceso IP para definir las direcciones locales internas para las cuales se aplica NAT. El comando ip nat pool muestra el primer y último números de un rango de direcciones globales internas. Por ejemplo, si el almacén necesitase diez direcciones, el comando podría haber indicado 200.1.1.1 y 200.1.1.10. El parámetro obligatorio netmask efectúa una especie de verificación del rango de direcciones. Si el rango de direcciones no va a estar en la misma subred, suponiendo que se utilizase el valor de netmask empleado en la configuración, entonces el IOS rechazará el comando ip nat pool. En este caso, la subred 200.1.1.0 y la máscara 255.255.255.252 (que es el valor especificado como netmask) incluirían a 200.1.1.1 y 200.1.1.2 en el rango de direcciones válidas, así que el IOS admite este comando.

Al igual que la NAT estática, la NAT dinámica utiliza el comando ip nat inside source. A diferencia de la NAT estática, la versión de NAT dinámica de este comando se refiere al

Ejemplo 16.2. Configuración de NAT dinámica.

```
NAT# show running-config
!
! Se han omitido ciertas líneas por brevedad
!
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip nat inside
!
interface Serial0/0
 ip address 200.1.1.251 255.255.255.0
 ip nat outside
!
ip nat pool fred 200.1.1.1 200.1.1.2 netmask 255.255.255.252
ip nat inside source list 1 pool fred
!
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.1
! El comando siguiente muestra una línea vacía porque todavía
! no se han creado entradas dinámicamente.
NAT# show ip nat translations

NAT# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/0
Inside interfaces:
  Ethernet0/0
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool fred refcount 0
 pool fred: netmask 255.255.255.252
    start 200.1.1.1 end 200.1.1.2
    type generic, total addresses 2, allocated 0 (0%), misses 0
```

nombre del almacén de NAT que va a utilizar para las direcciones globales internas; en este caso, se trata de fred. También hace referencia a una ACL IP, que define la lógica coincidente con las direcciones IP locales internas. El comando `ip nat inside source list 1 pool fred` establece una correspondencia entre los hosts definidos por la ACL 1 y el almacén llamado fred, que ha sido creado mediante el comando `ip nat pool fred`.

El Ejemplo 16.2 termina con un par de comandos `show` que confirman que el router todavía no tiene ninguna entrada en la tabla de conversión de NAT. Al principio, los comandos `show ip nat translations` y `show ip nat statistics` no muestran nada, o una información de configuración mínima. En este momento, ninguno de los hosts, 10.1.1.1 ni 10.1.1.2,

ha enviado paquete alguno, y NAT no ha creado entradas dinámica en la tabla NAT ni ha traducido direcciones en paquete alguno.

El comando show ip nat statistics que hay al final del ejemplo muestra una información especialmente interesante para la resolución de problemas con dos contadores distintos que se denominan "misses" (fallos), y están resaltados en el ejemplo. La primera aparición de este contador cuenta el número de veces que aparece un paquete nuevo, necesita una entrada de NAT y no encuentra una. En ese momento, la NAT dinámica reacciona y construye una entrada. El segundo contador de fallos que hay al final de la salida del comando indica el número de fallos que hay en el almacén. Este contador sólo crece cuando la NAT dinámica intenta asignar una nueva entrada de la tabla NAT y no halla direcciones disponibles, así que el paquete no se puede traducir; esto dará lugar, posiblemente, a que el usuario no llegue a la aplicación.

Para ver el contador de fallos y otros datos interesantes adicionales, el Ejemplo 16.3 continúa el ejemplo que comenzaba en el Ejemplo 16.2. Este ejemplo muestra los resultados que se producen cuando los hosts 10.1.1.1 y 10.1.1.2 empiezan a crear conexiones TCP,

Ejemplo 16.3. Verificación del funcionamiento normal de NAT dinámica.

```
! A continuación se ejecutó un Telnet desde 10.1.1.1 hacia 170.1.1.1; no se muestra
!
NAT# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial0/0
Inside interfaces:
  Ethernet0/0
Hits: 69 Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool fred refcount 1
 pool fred: netmask 255.255.255.252
   start 200.1.1.1 end 200.1.1.2
   type generic, total addresses 2, allocated 1 (50%), misses 0
NAT# show ip nat translations
Pro    Inside global   Inside local   Outside local    Outside global
---    200.1.1.1       10.1.1.1       ---              ---
NAT# clear ip nat translation *

!
! A continuación se ejecutó un Telnet desde 10.1.1.2 hacia 170.1.1.1; no se muestra
!
NAT# show ip nat translations
Pro    Inside global   Inside local   Outside local    Outside global
---    200.1.1.1       10.1.1.2       ---              ---
!
```

(continúa)

Ejemplo 16.3. Verificación del funcionamiento normal de NAT dinámica *(continuación).*

```
! A continuación se ejecutó un Telnet desde 10.1.1.1 hacia 170.1.1.1; no se muestra
!
NAT# debug ip nat
IP NAT debugging is on

01:25:44: NAT: s=10.1.1.1->200.1.1.2, d=170.1.1.1 [45119]
01:25:44: NAT: s=170.1.1.1, d=200.1.1.2->10.1.1.1 [8228]
01:25:56: NAT: s=10.1.1.1->200.1.1.2, d=170.1.1.1 [45120]
01:25:56: NAT: s=170.1.1.1, d=200.1.1.2->10.1.1.1 [0]
```

en este caso mediante Telnet. Este ejemplo prosigue en el momento en que finalizaba el Ejemplo 16.2.

El ejemplo comienza cuando el host 10.1.1.1 hace un telnet a 170.1.1.1 (que no se muestra), y el router NAT crea una entrada de NAT. La tabla NAT muestra una sola entrada, que asigna 10.1.1.1 a 200.1.1.1. Obsérvese que el primer contador de fallos que hay en el comando show ip nat statistics muestra 1 fallo, lo cual significa que hubo un primer paquete de la conexión TCP del host 10.1.1.1 a 170.1.1.1, y ese paquete dio lugar a que el router no encontrase una entrada en la tabla NAT, produciendo un incremento del contador. El contador de fallos que hay al final de la salida no se ha incrementado, porque el router pudo asignar un miembro del almacén y añadir una entrada a la tabla NAT. Obsérvese también que la última línea muestra estadísticas relativas al número de miembros del almacén que han sido asignados (1) y al porcentaje del almacén que se está utilizando actualmente (el 50%).

La tabla NAT se considera caducada al cabo de cierto periodo de inactividad. Sin embargo, para sacar forzosamente a una entrada de la tabla, se puede utilizar el comando clear ip nat translation*. Según se muestra en la Tabla 16.7 que hay al final del capítulo, este comando tiene algunas variantes. El Ejemplo 16.3 emplea la opción de fuerza bruta (clear ip nat translation*) que descarta todas y cada una de las entradas que haya en la tabla NAT dinámica. El comando también puede borrar entradas individuales, indicando las direcciones IP.

Tras borrar la entrada NAT, el host 10.1.1.2 hace telnet a 170.1.1.1. El comando show ip nat translations muestra ahora una correspondencia entre 10.1.1.2 y 200.1.1.1. Como 200.1.1.1 ya no está reservada en la tabla NAT, el router NAT puede reservarla para la próxima solicitud de NAT. (El IOS de Cisco tiende a seleccionar la dirección IP más baja disponible cuando selecciona la próxima dirección IP del almacén.)

Por último, al final del Ejemplo 16.3 se observa que el host ha hecho telnet a otro host de Internet, y se muestra también la salida del comando debug ip nat. Este comando debug da lugar a que el router mande un mensaje cada vez que se traduce la dirección de un paquete mediante NAT. Los resultados se generan insertando unas cuantas líneas de la conexión Telnet efectuada desde 10.1.1.1 hasta 170.1.1.1. Obsérvese que el resultado implica una conversión de 10.1.1.1 a 200.1.1.2, pero no implica conversión alguna de la dirección externa.

Configuración de sobrecarga NAT (PAT)

La sobrecarga de NAT, según se ha indicado anteriormente, permite a NAT soportar muchas direcciones IP locales internas con sólo una o unas pocas direcciones IP globales internas. En esencia, se convierten la dirección IP privada y el número de puerto a una sola dirección global interna, pero con un número de puerto exclusivo; esto permite a NAT soportar muchos hosts privados (más de 65000) con una sola dirección global pública.

En el IOS existen dos variantes de configuración de PAT. Si PAT utiliza un almacén de direcciones globales internas, la configuración tiene exactamente el mismo aspecto que una NAT dinámica, salvo que el comando global `ip nat inside source list` tiene la palabra reservada `overload` al final. Si PAT sólo necesita utilizar una dirección IP global interna, PAT puede utilizar una de sus direcciones IP de interfaz. Como NAT puede admitir más de 65000 flujos concurrentes con una sola dirección global interna, una sola dirección IP pública puede soportar las necesidades de NAT de toda una organización.

La lista de comprobación siguiente muestra detalladamente la configuración que hay que hacer cuando se emplea un almacén NAT:

Se utilizan los mismos pasos que para configurar una NAT dinámica, como se indicaba en la sección anterior, pero se incluye la palabra reservada `overload` al final del comando global `ip nat inside source list`.

La siguiente lista de comprobación muestra detalladamente la configuración que hay que efectuar cuando se utiliza una dirección IP de interfaz como única dirección IP global interna:

Paso 1 Al igual que en el caso de NAT estática y dinámica, se configuran las interfaces internas con el subcomando de interfaz `ip nat inside`.

Paso 2 Al igual que en el caso de NAT estática y dinámica, se configuran las interfaces externas con el subcomando de interfaz `ip nat outside`.

Paso 3 Al igual que en NAT dinámica, se configura una ACL que admite los paquetes que provengan de interfaces internas.

Paso 4 Se configura el comando de configuración global `ip nat source list` *número-de-acl* `interface` *número-o-nombre-de-interfaz* `overload`, que hace alusión a la ACL creada en el Paso 3 y a la interfaz cuya dirección IP se utilizará para las conversiones.

El Ejemplo 16.2 muestra una configuración de NAT dinámica. Para convertirla en una configuración de PAT, se utilizaría en su lugar el comando `ip nat inside source list pool fred overload`, añadiendo simplemente la palabra reservada `overload`.

El ejemplo siguiente muestra una configuración de PAT empleando una sola dirección IP de interfaz. La Figura 16.10 muestra la red ya conocida, con unos pocos cambios. En este caso, el ISP ha otorgado a FredsCo un subconjunto de la red 200.1.1.0: subred de CIDR 200.1.1.248/30. En otras palabras, esta subred tiene dos direcciones utilizables: 200.1.1.249 y 200.1.1.250. Estas direcciones se utilizan en ambos extremos del enlace serie que hay

entre FredsCo y su ISP. La característica NAT que hay en el router de FredsCo traduce todas las direcciones NAT a su dirección IP serie, 200.1.1.249.

En el Ejemplo 16.4, que muestra la configuración de sobrecarga de NAT, la NAT traduce empleando únicamente la dirección global interna 200.1.1.249, así que el almacén NAT no se necesita. En el ejemplo, según implica la Figura 16.10, el host 10.1.1.1 crea dos conexiones Telnet, y el host 10.1.1.2 crea una conexión Telnet, dando lugar a tres entradas de NAT dinámica, cada una de las cuales utiliza la dirección global interna 200.1.1.249, pero cada cual con su propio número de puerto.

Ejemplo 16.4. Configuración de sobrecarga NAT.

```
SNAT# show running-config
!
! Se han omitido líneas para abreviar
!
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip nat inside
!
interface Serial0/0
 ip address 200.1.1.249 255.255.255.252
 ip nat outside
!
ip nat inside source list 1 interface Serial0/0 overload
!
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.1
!

NAT# show ip nat translations
Pro   Inside global      Inside local     Outside local    Outside global
tcp   200.1.1.249:3212   10.1.1.1:3212    170.1.1.1:23     170.1.1.1:23
tcp   200.1.1.249:3213   10.1.1.1:3213    170.1.1.1:23     170.1.1.1:23
tcp   200.1.1.249:38913  10.1.1.2:38913   170.1.1.1:23     170.1.1.1:23
NAT# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:
  Serial0/0
Inside interfaces:
  Ethernet0/0
Hits: 103 Misses: 3
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 interface Serial0/0 refcount 3
```

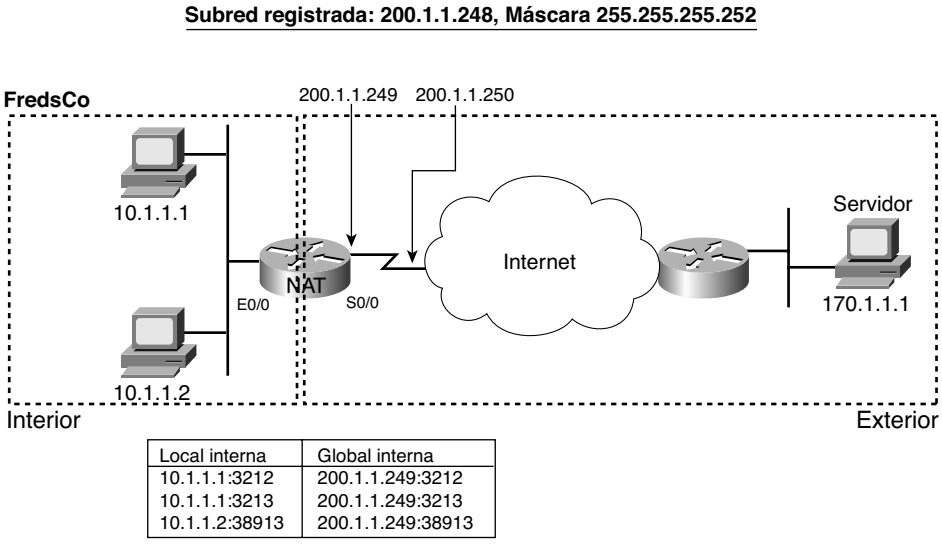


Figura 16.10. Sobrecarga de NAT yPAT.

El comando ip nat inside source list 1 interface serial 0/0 overload tiene varios parámetros, pero si se comprende la configuración de NAT dinámica, los nuevos parámetros no deberían ser demasiado difíciles de entender. El parámetro list 1 significa lo mismo que en NAT dinámica: las direcciones IP locales internas que indica la ACL 1 sufren una conversión de sus direcciones. El parámetro interface serial 0/0 significa que la única dirección IP global interna disponible es la dirección IP de la interfaz serie del router NAT 0/0. Por último, el parámetro overload significa que está activada la sobrecarga. Sin este parámetro, el router no lleva a cabo la sobrecarga, sólo utiliza NAT dinámica.

Como puede verse en la salida del comando show ip nat translations, se han añadido tres conversiones a la tabla NAT. Antes de este comando, el host 10.1.1.1 crea dos conexiones Telnet hasta 170.1.1.1, y el host 10.1.1.2 crea una sola conexión Telnet. Se crean tres entradas, una por cada combinación exclusiva de dirección IP local interna y número de puerto.

Resolución de problemas de NAT

Las tres partes principales de este libro dedican todo un capítulo a la resolución de problemas. En cada una de esas partes, los capítulos abordan toda una gama de temas relacionados con los temas técnicos tratados en cada capítulo. Los capítulos de resolución de problemas (el 3, el 7 y el 11) explican detalles relativos a la resolución de problemas con cada aspecto de la tecnología, y también sirven de ayuda para relacionar entre sí algunos conceptos.

La mayor parte de los problemas de NAT están relacionados con llegar a una configuración correcta. La lista siguiente resume unos cuantos consejos y pistas para resolver los problemas más frecuentes en la configuración de NAT. Después de la lista, el texto explica

un problema frecuente de enrutamiento que puede impedir que funcione NAT, y que está relacionado sobre todo con asegurarse de que la configuración sea correcta.

- Asegúrese de que la configuración incluye el subcomando de interfaz ip nat inside o ip nat outside. Estos subcomandos habilitan la NAT en las interfaces, y hay que distinguir entre inside y outside.
- Para configurar una NAT estática, asegúrese de que el comando ip nat source static contiene primero la dirección local interna, y en segundo lugar la dirección IP global interna.
- Para usar NAT dinámica, asegúrese de que la ACL configurada para admitir paquetes enviados por el host interno permite realmente el paso de esos paquetes antes de que se haya producido la traducción de NAT. Por ejemplo, si es preciso traducir la dirección local interna 10.1.1.1 a 200.1.1.1, asegúrese de que la ACL admite la dirección de origen 10.1.1.1, y no 200.1.1.1.
- Para utilizar NAT dinámica sin PAT, asegúrese de que el almacén contenga un número suficiente de direcciones IP. Entre los síntomas de no tener suficientes direcciones se incluye un valor creciente en el segundo contador de fallos en la salida del comando show ip nat statistics, así como ver todas las direcciones del rango definido en el almacén NAT dentro de la lista de conversiones dinámicas.
- En el caso de utilizar PAT, es fácil olvidarse de añadir la opción overload en el comando ip nat inside source list. Sin ella, NAT funciona pero PAT no, lo cual suele dar lugar a que no se traduzcan los paquetes de los usuarios, y entonces los hosts no pueden acceder a Internet.
- Quizás NAT esté bien configurado pero puede existir una ACL en una de las interfaces, lo cual da lugar a que se descarten los paquetes. Obsérvese que el IOS procesa las ACLs antes que NAT para los paquetes que entran en una interfaz, y después de traducir las direcciones de los paquetes para aquellos paquetes que salen de una interfaz.

Por último, la función NAT en un router puede verse afectada por un problema de enrutamiento que se produzca en otro router. Los routers que se hallan en la parte exterior de la red, frecuentemente en Internet, necesitan poder enrutar paquetes hacia direcciones IP globales internas que estén configuradas en el router NAT. Por ejemplo, en la Figura 16.4 vista anteriormente en este capítulo, se muestra el flujo de paquetes que van del interior al exterior, y del exterior al interior. Si nos centramos en el flujo desde el exterior hasta el interior, los routers de Internet necesitan saber la forma de enrutar paquetes a la dirección IP registrada y pública 200.1.1.1. Normalmente, este rango de direcciones sería notificado por un protocolo de enrutamiento dinámico. Por tanto, si una revisión de la configuración de NAT muestra que la configuración parece correcta, examine las rutas que hay tanto en el router NAT como en otros routers, para asegurarse de que los routers pueden reenviar los paquetes basándose en las direcciones empleadas en ambos lados del router que lleva a cabo la función NAT.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 16.5 específica estos temas y el número de la página en la que se encuentra cada uno. Además, obsérvese que las listas de comprobación de configuración deben revisarse y estudiarse para conocer su contenido, pero no es necesario memorizar el número de cada paso, ni su orden; son solamente herramientas cómodas para recordar todos los pasos.

Tabla 16.5. Temas clave del Capítulo 16.

Tema clave	Descripción	Número de página
Figura 16.1	Concepto de asignación de dirección IPv4 global CIDR, y de agregación de rutas.	554
Tabla 16.2	Lista de números de red IP privadas.	556
Figura 16.2	Concepto principal de NAT como conversión de direcciones IP privadas a direcciones globales exclusivas públicamente.	557
Figura 16.4	Diagrama típico de una red con NAT, mostrando los términos clave de NAT.	558
Tabla 16.3	Lista de cuatro términos clave de NAT y de sus significados.	559
Figura 16.7	Conceptos que subyacen a la conservación de direcciones que se logra por sobrecarga de NAT (PAT).	563
Lista	Lista de comprobación para la configuración de NAT estática.	565-566
Lista	Lista de comprobación para la configuración de NAT dinámica.	568
Lista	Resumen de las diferencias que existen entre la configuración de NAT dinámica y de PAT empleando un almacén.	572
Lista	Lista de comprobación para la configuración de PAT empleando la dirección IP de una interfaz.	572
Lista	Errores más frecuentes en NAT.	575

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD) o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo y compruebe sus respuestas en el glosario:

CIDR, global externa, global interna, local externa, local interna, PAT, red IP privada, sobrecarga de NAT.

Referencias de comandos

Aunque no necesariamente debe memorizar la información de las tablas de esta sección, ésta incluye una referencia de los comandos de configuración y EXEC utilizados en este capítulo. En la práctica, debería memorizar los comandos como un efecto colateral de leer el capítulo y hacer todas las actividades de esta sección de preparación del examen. Para verificar si ha memorizado los comandos como un efecto colateral de sus otros estudios, cubra el lado izquierdo de la tabla con un pedazo de papel, lea las descripciones del lado derecho y compruebe si recuerda el comando.

Tabla 16.6. Comandos de configuración del Capítulo 16.

Comando	Descripción
ip nat {inside | outside}	Subcomando de interfaz que activa NAT e identifica si la interfaz está en el interior o el exterior de la red.
ip nat inside source {list {*número-de-lista-de-acceso* | *nombre-de-lista-de-acceso*}} {interface *tipo número* | pool *nombre-almacén*} [overload]	Comando global que activa NAT globalmente, haciendo referencia a la ACL que define qué direcciones de origen han de convertirse, y la interfaz o almacén en el que se hallarán direcciones globales.
ip nat pool *nombre ip-inicial ip-final* {netmask *máscara* | prefix-length l*ongitud-prefijo*}	Comando global que define un almacén de direcciones NAT.

Tabla 16.7. Comandos EXEC del Capítulo 16.

Comando	Descripción
show ip nat statistics	Muestra los contadores de paquetes y las entradas de la tabla NAT, así como información básica sobre la configuración.
show ip nat translations [verbose]	Muestra la tabla NAT.
clear ip nat translation {* | [inside *ip-global ip-local*] [outside *ip-local ip-global*]}	Borra las entradas dinámicas que hay en la tabla NAT (todas o algunas), dependiendo de los parámetros que se utilicen.
clear ip nat translation *protocolo* inside *ip-global puerto-global ip-local puerto-local* [outside *ip-local ip-global*]	Borra algunas de las entradas dinámicas de la tabla NAT, dependiendo de los parámetros que se utilicen.
debug ip nat	Emite un mensaje de registro que describe todos los paquetes cuya dirección IP haya sido traducida por NAT.

Este capítulo trata los siguientes temas:

Direccionamiento de unidifusión global, enrutamiento y subredes: Esta sección presenta los conceptos que subyacen a las direcciones IPv6 de unidifusión, al enrutamiento IPv6, y a la creación de subredes utilizando IPv6, comparándolo todo con IPv4.

Protocolos y direccionamiento IPv6: Esta sección estudia los protocolos de uso más frecuente en IPv6.

Configuración del enrutamiento y de los protocolos de enrutamiento en IPv6: Esta sección muestra la forma de configurar el enrutamiento y los protocolos de enrutamiento IPv6 en routers de Cisco.

Opciones para la transición a IPv6: Esta sección explica algunas de las opciones existentes para migrar de IPv4 a IPv6

CAPÍTULO 17

IP Versión 6

La versión 6 de IP (IPv6), que es el protocolo que sustituirá a IPv4, es bien conocida por un par de razones. IPv6 ofrece la solución final para el problema de quedase sin direcciones IPv4 en la Internet global, empleando una dirección de 128 bits; esto son aproximadamente 10^{38} direcciones en total, frente a tan sólo (aproximadamente) $4*10^9$ direcciones totales en IPv4. Sin embargo, IPv6 lleva siendo la solución final a largo plazo desde hace más de diez años, en parte como consecuencia de soluciones para el ínterin, entre las que se cuenta la Conversión de direcciones de red y la Conversión de direcciones de puerto (NAT/PAT), que afortunadamente han retrasado el día en que realmente se agoten las direcciones IP de unidifusión públicas.

Este capítulo se centra en el direccionamiento y el enrutamiento IPv6, en parte porque la motivación primaria para la eventual migración a IPv6 es aliviar las restricciones de direcciones que impone IPv4. Este capítulo también presenta brevemente algunas de las otras características de IPv6, y también explica algunas de las razones por las cuales se necesita IPv6.

Cuestionario "Ponga a prueba sus conocimientos"

El cuestionario "Ponga a prueba sus conocimientos" le permite evaluar si debe leer el capítulo entero. Si sólo falla una de las nueve preguntas de autoevaluación, podría pasar a la sección "Ejercicios para la preparación del examen". La Tabla 17.1 especifica los encabezados principales de este capítulo y las preguntas del cuestionario que conciernen al material proporcionado en ellos para que de este modo pueda evaluar el conocimiento que tiene de estas áreas específicas. Las respuestas al cuestionario aparecen en el Apéndice A.

1. ¿Cuál de las siguientes es la organización que podría otorgar a una empresa una asignación administrativa de un bloque de direcciones IP de unidifusión global IPv6?

a. Un ISP

b. ICANN

c. Un RIR

Tabla 17.1. Relación entre las preguntas del cuestionario y los temas fundamentales del capítulo.

Sección de Temas fundamentales	Preguntas
Direccionamiento de unidifusión global, enrutamiento y subredes	1-2
Protocolos y direccionamiento IPv6	3-5
Configuración del enrutamiento y de los protocolos de enrutamiento en IPv6	6-8
Opciones para la transición a IPv6	9

d. Las direcciones de unidifusión no son asignadas administrativamente por una organización externa.

2. ¿Cuál de las siguientes es la abreviatura válida más corta de FE80:0000:0000:0100:0000:0000:0000:0123?

a. FE80::100::123

b. FE8::1::123

c. FE80::100:0:0:0:123:4567

d. FE80:0:0:100::123

3. ¿Cuál de las siguientes respuestas muestra una dirección IPv6 de multidifusión?

a. 2000::1:1234:5678:9ABC

b. FD80::1:1234:5678:9ABC

c. FE80::1:1234:5678:9ABC

d. FF80::1:1234:5678:9ABC

4. ¿Cuál de las siguientes respuestas muestra o un protocolo o una función que un host pueda utilizar para aprender dinámicamente sus propias direcciones IPv6?

a. DHCP con estado.

b. DHCP sin estado.

c. Autoconfiguración sin estado.

d. Protocolo de descubrimiento de vecinos (*Neighbor Discovery Protocol*).

5. ¿Cuáles de los siguientes conceptos sirven de ayuda a un host IPv6 para aprender la dirección IP de un gateway predeterminado en su propia subred?

a. DHCP con estado.

b. DHCP sin estado.

c. Autoconfiguración sin estado.

d. Protocolo de descubrimiento de vecinos (*Neighbor Discovery Protocol*).

6. ¿Cuáles de los siguientes son protocolos de enrutamiento que soportan IPv6?
   a. RIPng
   b. RIP-2
   c. OSPFv2
   d. OSPFv3
   e. OSPFv4
7. En la configuración siguiente, la interfaz Fa0/0 de este router tiene la dirección MAC 4444.4444.4444. ¿Cuál de las direcciones IPv6 siguientes utilizará la interfaz?

```
ipv6 unicast-routing
ipv6 router rip tag1
interface FastEthernet0/0
 ipv6 address 3456::1/64
```

   a. 3456::C444:44FF:FE44:4444
   b. 3456::4444:44FF:FE44:4444
   c. 3456::1
   d. FE80::1
   e. FE80::6444:44FF:FE44:4444
   f. FE80::4444:4444:4444
8. En el texto de configuración de la pregunta anterior, RIP no estaba operativo en la interfaz Fa0/0. ¿Cuál de los siguientes comandos de configuración habilitaría RIP en Fa0/0?
   a. network 3456::/64
   b. network 3456::/16
   c. network 3456::1/128
   d. ipv6 rip enable
   e. ipv6 rip tag1 enable
9. ¿Cuáles de los siguientes métodos de transición de IPv4 a IPv6 permiten que un host que sólo soporta IPv4 se comunique con un host que sólo soporta IPv6?
   a. Pila dual
   b. Un túnel 6to4
   c. Un túnel ISATAP
   d. NAT-PT

Temas fundamentales

El mundo ha experimentado un tremendo cambio a lo largo de los 10 ó 20 últimos años, como resultado del crecimiento y la maduración de Internet y de las tecnologías de redes

en general. Hace veinte años no existía una red global a la que el público en general pudiera conectarse fácilmente. Hace diez años, la Internet pública había crecido hasta el punto en que la gente de la mayor parte del mundo podía conectarse a Internet, pero la mayoría de los usuarios eran personas relacionadas con el mundo de la computación. En la actualidad, todo el mundo parece tener acceso, mediante sus PCs, PDAs, teléfonos y hasta el refrigerador.

La eventual migración a IPv6 se verá impulsada, probablemente, por la necesidad de disponer de más direcciones. Casi todos los teléfonos móviles admiten Internet, y esto requiere el uso de una dirección IP. La mayoría de los coches nuevos tienen la capacidad de adquirir y utilizar una dirección IP, y además disponen de comunicaciones inalámbricas, lo cual permite al concesionario ponerse en contacto con el cliente cuando los diagnósticos del coche detectan un problema. Algunos fabricantes han adoptado ya esta idea, y todos sus dispositivos necesitan tener una IP habilitada.

Además del mero crecimiento de la necesidad de direcciones IPv4, la normativa gubernamental podría impulsar la demanda de IPv6. En el momento de escribir estas líneas, el gobierno de los Estados Unidos de América ha fijado una fecha de 2008 para que todos y cada uno de sus organismos esté utilizando IPv6 en sus redes IP esenciales. Estas iniciativas podrían acelerar la adopción de IPv6.

Aunque las dos mayores razones por las cuales las redes podrían migrar a IPv6 son la necesidad de más direcciones y los mandatos de los gobiernos, también es cierto que IPv6 ofrece algunas características atractivas, y también herramientas para la migración. Entre las ventajas que aporta cabe mencionar las siguientes:

- **Características de asignación de direcciones:** la asignación de direcciones IPv6 permite cambios más fáciles en la numeración, asignación dinámica y recuperación de direcciones, con características agradables para que los dispositivos móviles se trasladen y mantengan sus direcciones IP (evitando, por tanto, la necesidad de cerrar y volver a abrir las aplicaciones).
- **Agregación:** el enorme espacio de direcciones de IPv6 hace mucho más sencilla la agregación de bloques de direcciones en Internet.
- **No se necesita NAT/PAT:** al emplear direcciones exclusivas registradas públicamente en todos los dispositivos, se elimina la necesidad de NAT/PAT, lo cual evita también parte de los problemas de la capa de aplicación y de los túneles VPN que causa el uso de NAT.
- **IPsec:** IPsec funciona tanto con IPv4 como con IPv6, pero es obligatoria en los hosts IPv6, así que puede uno basarse en el soporte de IPsec cuando éste resulta necesario para el *tunneling* VPN.
- **Mejoras de los encabezados:** aunque pueda parecer una cuestión sin importancia, el encabezado de IPv6 mejora varias cosas en comparación con IPv4. En particular, los routers no necesitan recalcular la suma de comprobación del encabezado para cada paquete, lo cual reduce el coste por paquete. Además, el encabezado incluye una etiqueta de flujo que permite identificar fácilmente los paquetes que se mandan a través de una misma conexión TCP o UDP.

- **Herramientas para la transición:** según se describe en la última sección principal de este capítulo, IPv6 posee muchas herramientas que sirven de ayuda para efectuar la transición de IPv4 a IPv6.

La migración mundial de IPv4 a IPv6 no será un evento, ni un año del calendario. Será, más bien, un proceso largo, un proceso que ya ha comenzado. Los ingenieros de redes tienen una necesidad cada vez mayor de aprender más sobre IPv6. Este capítulo abarca las bases de IPv6, y termina con algunas descripciones de los problemas asociados a vivir en un mundo en el que IPv4 e IPv6 tienen grandes probabilidades de coexistir durante bastante tiempo.

Nota

Information Week (http://www.informationweek.com) ha publicado un interesante artículo sobre la necesidad de migrar a IPv6 en el momento en que se estaba poniendo punto final al libro. Para ver el artículo, busque en este sitio web el artículo titulado "The Impending Internet Address Shortage" (La carestía de direcciones de Internet que se avecina).

Direccionamiento de unidifusión global, enrutamiento y subredes

Uno de los objetivos de diseño originales de Internet fue que todas las organizaciones se registrasen y les fueran asignadas una o más redes IP públicas (de Clase A, B o C). Al registrarse para utilizar un número de red pública en particular, la compañía o la organización que utilizase esa red tendría la seguridad (otorgada por las autoridades de numeración) de que ninguna otra compañía u organización del mundo utilizaría las direcciones de esa red. Como resultado, todos los hosts del mundo dispondrían de una dirección IP exclusiva globalmente.

Desde la perspectiva de la infraestructura de Internet, y en particular con el objetivo de evitar que las tablas de enrutamiento de Internet se hicieran demasiado grandes, la asignación de toda una red a cada organización era hasta cierto punto una ayuda. Los routers de Internet podían ignorar las subredes, teniendo en su lugar una ruta por cada red completa. Por ejemplo, si a una compañía registrada se le asignaba la red de Clase B 128.107.0.0/16, los routers de Internet sólo necesitarían una ruta para toda esa red.

Con el paso del tiempo, Internet creció enormemente. A principios de la década de los 90 estaba claro que habría que hacer algo, o bien el crecimiento de Internet se detendría estrepitosamente cuando todas las redes IP públicas estuvieran asignadas y no hubiera ninguna más. Además, las tablas de enrutamiento IP que había en los routers de Internet se estaban volviendo demasiado grandes para la tecnología de routers de la época. Por tanto, la comunidad de Internet se puso a trabajar para inventar soluciones a corto y largo plazo para los dos problemas: la falta de direcciones públicas y el tamaño de las tablas de enrutamiento.

Entre las soluciones a corto plazo se contaba una política de asignación de direcciones públicas mucho más inteligente, en que las direcciones públicas no se asignaban sólo como redes de Clase A, B y C, sino formando subdivisiones más pequeñas (prefijos), reduciendo así el desperdicio. Además, el crecimiento de las tablas de enrutamiento de Internet se redujo mediante una asignación más inteligente de los rangos de direcciones. Por ejemplo, al asignar las redes de Clase C que empiezan por 198 a un solo proveedor de servicios de Internet (ISP) de una cierta zona del mundo se permitía que otros ISPs utilizasen una ruta para 198.0.0.0/8 (en otras palabras, para todas las direcciones que empiezan por 198) en lugar de tener una ruta para cada una de las 65536 redes de Clase C distintas que comienzan por 198. Por último, NAT/PAT lograban resultados asombrosos al permitir que un hogar o una pequeña oficina consumieran únicamente una dirección IPv4 pública, reduciendo de ese modo enormemente la necesidad de direcciones IPv4 públicas.

La solución final de ambos problemas es IPv6. El número total de direcciones de IPv6 resuelve el problema de agotar las direcciones. Las políticas de asignación de direcciones que ya se utilizaban con IPv4 se han refinado y aplicado a IPv6, con buenos resultados para mantener el tamaño de las tablas de enrutamiento IPv6 más reducido en los routers de Internet. Las secciones siguientes ofrecen una descripción general de ambos problemas, y en particular de la forma en que las direcciones de unidifusión globales, junto con unas buenas decisiones administrativas relativas a la asignación de prefijos en las direcciones de IPv6, sirven de ayuda para el enrutamiento en la Internet global. Estas secciones concluyen con una descripción del uso de subredes en IPv6.

Agregación global de rutas para un enrutamiento eficiente

En la época en la que se estaba definiendo IPv6, a principios de la década de los 90, estaba claro que una cuidadosa selección de la forma de reservar el espacio de direcciones públicas de IPv4 podría mejorar la eficiencia de los routers de Internet, haciendo que sus tablas de enrutamiento fueran mucho más reducidas. Al emplear estas lecciones tan bien aprendidas, la asignación de direcciones IP públicas en IPv6 puede producir un enrutamiento aún más eficiente a medida que Internet va migrando a IPv6.

La estrategia de asignación de direcciones para IPv6 es elegante pero sencilla, y se puede resumir básicamente de esta forma:

- Las direcciones públicas de IPv6 están agrupadas (numéricamente) por grandes regiones geográficas.
- Dentro de cada región, el espacio de direcciones se subdivide a su vez por ISP dentro de esa región.
- Dentro de los ISPs de cada región, el espacio de direcciones se subdivide aún más para cada cliente.

Las organizaciones que manipulan esta asignación de direcciones para IPv6 son las mismas que lo hacen para IPv4. La *Internet Corporation for Assigned Network Numbers*

(ICANN, http://www.icann.org) es la propietaria del proceso. ICANN asigna uno o más intervalos de direcciones IPv6 a cada Registro regional de Internet (*Regional Internet Registry*, RIR), de los cuales hay cinco en el momento de escribir estas líneas, que abarcan aproximadamente América del Norte, América Central y del Sur, Europa, Asia y el Pacífico, y África. Estos RIRs, a su vez, subdividen su espacio de direcciones asignado en partes más pequeñas, y asignan prefijos a diferentes ISPs y a otros registros más pequeños; después, los ISPs asignan rangos todavía más pequeños de direcciones a sus clientes.

Nota

La *Internet Assigned Numbers Authority* (IANA) era quien poseía anteriormente el proceso de asignación de direcciones, pero su responsabilidad se ha traspasado a ICANN.

El plan de asignación de direcciones globales IPv6 da lugar a un enrutamiento más eficiente, como puede verse en la Figura 17.1. La figura muestra una compañía ficticia (Empresa1) a la que le ha sido asignado un prefijo IPv6 por parte de un ISP ficticio, NA-ISP1 (que quiere decir ISP norteamericano número 1). La figura muestra el Registro americano para los números de Internet (*American Registry for Internet Numbers*, ARIN), que es el RIR de América del Norte.

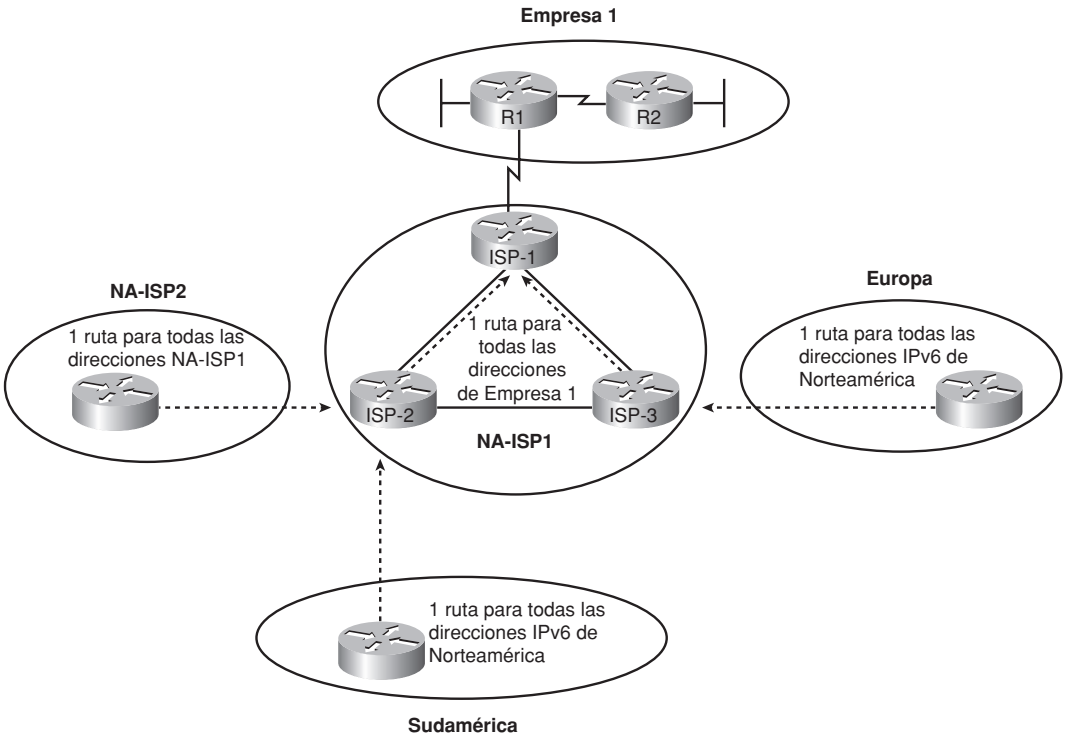


Figura 17.1. Visión conceptual de las rutas globales de IPv6.

Como se muestra en la figura, los routers instalados por ISPs de otras zonas geográficas pueden tener una sola ruta que denota todas las direcciones de Norteamérica. Aunque puede haber centenares de ISPs operando en Norteamérica, y cientos de miles de clientes comerciales de esos ISPs, y decenas de millones de clientes individuales, todas las direcciones públicas de IPv6 pueden ser de un bloque muy grande de direcciones, o de unos pocos, y esto requerirá tan solo una ruta (o unas pocas) en los routers de Internet de otras partes del mundo. De forma similar, los routers situados dentro de otros ISPs de Norteamérica (por ejemplo, NA-ISP2, que denota el ISP número 2 de Norteamérica en la figura) pueden tener una ruta que denote todos los rangos de direcciones asignados a NA-ISP2. Y los routers situados dentro de NA-ISP1 sólo necesitan tener una ruta que denote todo el rango de direcciones asignado a Empresa1, en lugar de necesitar saberlo todo sobre las subredes existentes dentro de Empresa1.

Además de mantener una tabla de enrutamiento mucho más pequeña en los routers, este proceso también da lugar a menos cambios en las tablas de enrutamiento de los routers de Internet. Por ejemplo, si firmase un contrato de servicio con otro cliente de tipo empresarial, NA-ISP1 podría asignarle otro prefijo situado dentro del rango de direcciones que ya han sido asignadas a NA-ISP1 por parte de ARIN. Los routers situados fuera de la red de NA-ISP1 (esto es, la mayor parte de Internet) no necesitan conocer nuevas rutas, porque sus rutas ya existentes denotan ya el rango de direcciones que está asignado al nuevo cliente. Los routers de NA-ISP2 (que es otro ISP) ya tienen una ruta que denota todo el rango de direcciones completo que ha sido asignado a NA-ISP1, así que no necesitan ninguna ruta más. De forma análoga, los routers de los ISPs situados en Europa y Sudamérica ya tienen una ruta que funciona perfectamente.

Aunque el concepto general puede no ser demasiado difícil, un ejemplo concreto servirá de ayuda. Antes de ver un ejemplo concreto, también viene bien conocer un poquito la forma en que se escriben las direcciones y prefijos de IPv6.

Convenciones para la representación de direcciones IPv6

Las convenciones de IPv6 utilizan 32 números hexadecimales, organizados en 8 cuartetos de 4 dígitos hexadecimales separados mediante dos puntos, para representar una dirección IPv6 de 128 bits. Por ejemplo:

2340:1111:AAAA:0001:1234:5678:9ABC

Cada dígito hexadecimal representa 4 bits, así que si se desea examinar la dirección en binario, la conversión es relativamente sencilla si se memorizan los valores mostrados en la Tabla 17.2.

Escribir o teclear 32 dígitos hexadecimales, aunque es más cómodo que hacer lo mismo con 128 dígitos binarios, sigue siendo engorroso. Para hacer las cosas un poco más sencillas, hay dos convenciones que nos permiten abreviar lo que es preciso escribir para una dirección IPv6:

Tabla 17.2. Tabla de conversión de hexadecimal a binario.

Hex	Binario	Hex	Binario
0	0000	8	1000
1	0001	9	1001
2	0010	A	1010
3	0011	B	1011
4	0100	C	1100
5	0101	D	1101
6	0110	E	1110
7	0111	F	1111

- Omitir los ceros iniciales de cualquier cuarteto.
- Representar uno o más cuartetos consecutivos formados por ceros hexadecimales en forma de dos signos de dos puntos (::), pero sólo para una instancia semejante en cada dirección.

Tema clave

Nota

Para IPv6, un cuarteto es un conjunto de 4 dígitos hexadecimales de una dirección IPv6. En toda dirección IPv6 hay ocho cuartetos.

Por ejemplo, considere la dirección siguiente. Los dígitos en negrita representan los dígitos en que se podría abreviar la dirección.

FE00:**0000**:**0000**:**000**1:**0000**:**0000**:**0000**:**00**56

Esta dirección tiene dos ubicaciones diferentes en las que uno o más cuartetos tienen cuatro ceros hexadecimales, así que existen dos opciones principales para abreviar esta dirección, empleando la abreviatura :: en una u otra ubicación. Las dos opciones siguientes muestran las dos abreviaturas válidas más cortas:

- FE00::1:0:0:0:56
- FE00:0:0:1::56

En particular, obsérvese que la abreviatura ::, que significa "uno o más cuartetos formados únicamente por ceros", no se puede utilizar dos veces porque sería ambigua. Por tanto, la abreviatura FE00::1::56 no sería válida.

Convenciones para escribir prefijos de IPv6

Los prefijos de IPv6 representan un rango o bloque de direcciones IPv6 consecutivas. El número que representa el rango de direcciones, que es lo que se llama **prefijo**, suele verse

en las tablas de enrutamiento IP, exactamente como se ven los números de subred IP en las tablas de enrutamiento IPv4.

Antes de examinar los prefijos IPv6 con más detalle, puede servir de ayuda revisar unos cuantos términos que se utilizan con IPv4. Las direcciones de IPv4 se pueden analizar y comprender empleando reglas de **direccionamiento con clase** o bien reglas de **direccionamiento sin clase**. (Tanto este libro como la guía ***CCENT/CCNA ICND1*** utilizan la terminología "con clase" en su mayor parte.) El direccionamiento con clase significa que el análisis de una dirección IP o de una subred incluye la idea de un número de red con clase, con una parte separada de la dirección que corresponde a la red. La parte superior de la Figura 17.2 revisa estos conceptos.

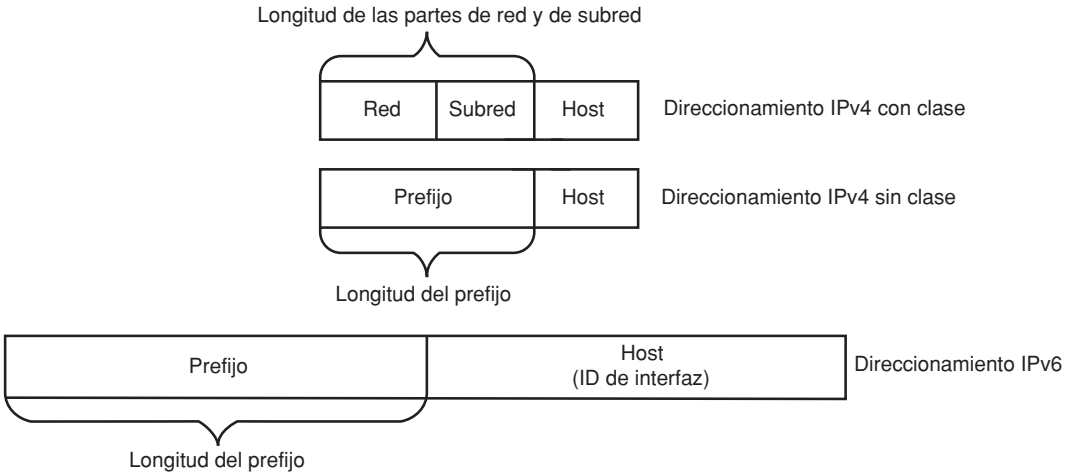


Figura 17.2. Direccionamiento IPv4 sin clase y con clase, y direccionamiento IPv6.

Al pensar en el direccionamiento IPv4 como direcciones con clase se entienden en su totalidad ciertos problemas de las redes. Por ejemplo, cuando se utiliza el direccionamiento con clase, el valor 128.107.3.0/24 significa 16 bits de red (porque la dirección se encuentra en una red de Clase B) y 8 bits de host (porque la máscara tiene 8 ceros binarios), y quedan 8 bits de subred. Este mismo valor, interpretado desde el punto de vista de las reglas sin clase, significa el prefijo 128.107.3.0, con longitud de prefijo 24. Es la misma subred y prefijo, el mismo significado, el mismo funcionamiento del router, la misma configuración; sólo son dos formas distintas de pensar en el significado de los números.

IPv6 utiliza un punto de vista sin clase del direccionamiento, sin tener un concepto de direccionamiento con clase. Al igual que IPv4, los prefijos de IPv6 muestra un cierto valor, una barra y después una longitud de prefijo numérica. Al igual que los prefijos de IPv4, la última parte del número, más allá de la longitud del prefijo, está representada por ceros binarios. Por último, los números de prefijo de IPv6 se pueden abreviar empleando las

mismas reglas que en las direcciones de IPv4. Por ejemplo, considere la siguiente dirección de IPv6 que se le ha asignado a un host de una LAN:

2000:1234:5678:9ABC:1234:5678:9ABC:1111/64

Este valor representa toda la dirección IP completa de 128 bits; de hecho, no hay forma de abreviar esta dirección. Sin embargo, el /64 significa que el prefijo (subred) en que reside esta dirección es la subred que incluye todas las subredes que comienzan por los mismos 64 bits que la dirección. Conceptualmente, es la misma lógica que en una dirección IPv4. Por ejemplo, la dirección 128.107.3.1/24 está en el prefijo (subred) cuyos primeros 24 bits son los mismos valores que en la dirección 128.107.3.1.

Igual que en IPv4, cuando se escribe o teclea un prefijo, los bits que están más allá de la longitud del prefijo son todos ellos ceros binarios. En la dirección IPv6 mostrada anteriormente, el prefijo en que reside la dirección sería el siguiente:

2000:1234:5678:9ABC:**0000:0000:0000:0000**/64

En forma abreviada sería:

2000:1234:5678:9ABC::/64

A continuación, un detalle más relativo a las reglas que se siguen para escribir prefijos antes de examinar algunos ejemplos y seguir adelante. Si la longitud del prefijo no es múltiplo de 16, entonces el límite entre el prefijo y la parte de host de la dirección se encuentra dentro de un cuarteto. En estos casos, el valor del prefijo debería enumerar todos los valores del último octeto en la parte de prefijo del valor. Por ejemplo, si la dirección que se ha mostrado con una longitud de prefijo de /64 tuviera una longitud de prefijo de /56, entonces el prefijo incluiría los tres primeros cuartetos en su totalidad (un total de 48 bits), más los 8 primeros bits del cuarto cuarteto. Los últimos 8 bits (los dos últimos dígitos hexadecimales) del cuarto octeto deberían ser ahora ceros binarios. Por tanto, por convención, el resto del cuarto octeto se debería escribir, después de darle como valor una colección de ceros binarios, de este modo:

2000:1234:5678:9A**00**::/56

La lista siguiente resume algunos puntos clave relativos a la forma de escribir prefijos de IPv6:

- El prefijo tiene los mismos valores que las direcciones IP del grupo para el primer número de bits, tal como está definido por la longitud del prefijo.
- Todos los bits que vayan después del número de longitud de prefijo de bits son ceros binarios.
- El prefijo se puede abreviar con las mismas reglas que las direcciones IPv6.
- Si la longitud del prefijo no está en el límite de un cuarteto, se escribe el valor del cuarteto entero.

Ciertamente, en este caso los ejemplos pueden ser de mucha ayuda. La Tabla 17.3 muestra varios prefijos, su formato y una breve explicación.

Casi igualmente importante para esta convención es tomar nota de las opciones que no se permiten. Por ejemplo, no se permite 2::/3 en lugar de 2000::/3, porque omite el resto

Tabla 17.3. Ejemplos de prefijos IPv6 y de sus significados.

Prefijo	Explicación	Alternativa incorrecta
2000::/3	Todas las direcciones cuyos tres primeros bits son iguales a los tres primeros bits del número hexadecimal 2000 (los bits son 001)	2000/3 (omite ::) 2::/3 (omite el resto del primer cuarteto)
2340:1140::/26	Todas las direcciones cuyos 26 primeros bits coinciden con el número hexadecimal indicado	2340:114::/26 (omite el último dígito del segundo cuarteto)
2340:1111::/32	Todas las direcciones cuyos 32 primeros bits coinciden con el número hexadecimal indicado	2340:1111/32 (omite el ::)

del octeto, y un dispositivo no podría decidir si 2::/3 significa "0002 en hexadecimal" o "2000 en hexadecimal". Cuando se abrevia una dirección o prefijo de IPv6 sólo se pueden omitir los ceros iniciales del cuarteto, y no los finales.

Una vez comprendidas algunas de las convenciones relativas a la representación de direcciones y prefijos de IPv6, un ejemplo concreto puede mostrar la forma en que la estrategia de asignación de direcciones IP de unidifusión globales de ICANN puede permitir el enrutamiento sencillo y eficiente que se mostraba en la Figura 17.1.

Ejemplo de asignación de un prefijo de unidifusión global

Los estándares de IPv6 reservan el prefijo 2000::/3 (que, cuando se interpreta más completamente, significa todas las direcciones que comienzan por un 001 binario o bien por un 2 o un 3 hexadecimal) como direcciones de unidifusión global. Las direcciones de unidifusión global son direcciones que están reservadas como direcciones IPv6 exclusivas, públicas y globalmente únicas, y que permiten a los hosts que emplean esas direcciones comunicarse a través de Internet sin necesidad de NAT. En otras palabras, estas direcciones encajan con el diseño más puro posible de la forma de implementar IPv6 para la Internet global.

La Figura 17.3 muestra un ejemplo de un conjunto de prefijos que podrían dar lugar a que a una compañía (Empresa1) se le asignase como prefijo el 2340:1111:AAAA::/48.

El proceso comienza con ICANN, que posee todo el espacio de direcciones completo de IPv6, y asigna los derechos de registrar el prefijo 2340::/12 a uno de los RIRs, que en este caso es ARIN (Norteamérica). Esto significa que ARIN posee los derechos de asignar cualquier dirección IPv6 que comience por los 12 primeros bits del número hexadecimal 2340

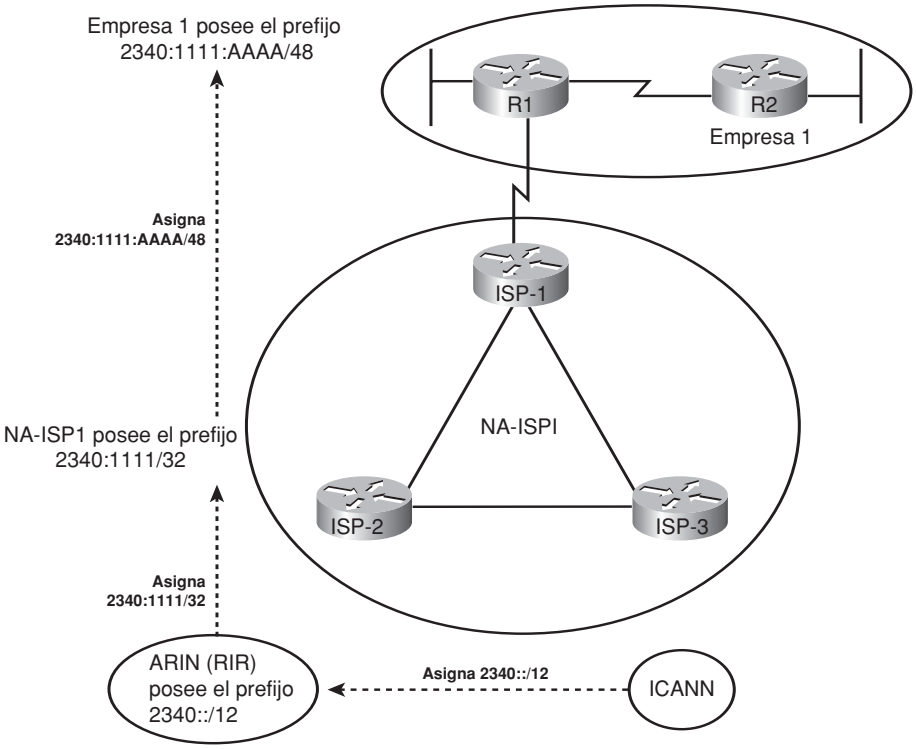


Figura 17.3. Ejemplo de asignación de prefijo IPv6 en Internet.

(cuyo valor binario es 0010 0011 0100). Para poner en perspectiva esta indicación, téngase en cuenta que se trata de un grupo muy grande de direcciones: 2^{116} para ser exactos.

A continuación, NA-ISP1 pide a ARIN la asignación de un prefijo. Una vez que ARIN se asegura de que NA-ISP1 cumple ciertos requisitos, ARIN puede asignar el **prefijo de ISP** 2340:1111::/32 a NA-ISP1. Se trata de un grupo exageradamente grande; son 2^{96} direcciones para ser exactos. Para poner en perspectiva esta indicación, este bloque de direcciones podría contener suficientes direcciones IPs públicas hasta para el más grande de los ISP, sin que ese ISP volviera a necesitar nunca otro prefijo de IPv6.

Por último, Empresa1 solicita a su ISP, NA-ISP1, la asignación de un prefijo IPv6. NA-ISPs asigna a Empresa1 el prefijo de sitio 2340:1111:AAAA::/48, que es, una vez más, un enorme rango de direcciones; en este caso son 2^{80}. En el prefijo siguiente el texto muestra lo que podría hacer Empresa1 con ese prefijo, pero examinemos primero la Figura 17.4, que representa los mismos conceptos que se muestran en la Figura 17.1, salvo que ahora ya se muestran los prefijos.

La figura muestra las perspectivas de los routers situados fuera de Norteamérica, de los routers de otro ISP situado en Norteamérica, y de otros routers situados en el mismo ISP. Los routers situados fuera de Norteamérica pueden utilizar una ruta para el prefijo 2340::/12, sabiendo que ICANN ha reservado ese prefijo para ser utilizado exclusivamen-

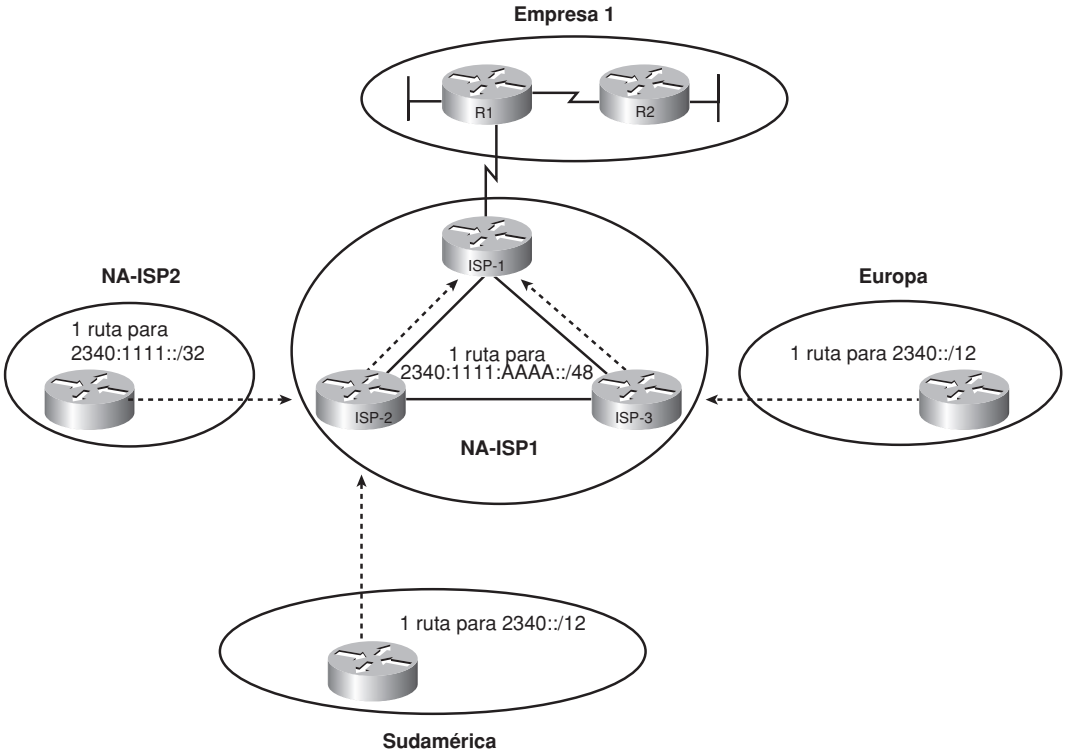


Figura 17.4. Conceptos de enrutamiento global en IPv6.

te por ARIN. Esta única ruta podría denotar todas las direcciones IPv6 asignadas en Norteamérica. Los routers de NA-ISP2, que es un ejemplo de ISP alternativo en Norteamérica, necesitan una ruta para 2340:1111::/32, que es el prefijo asignado a NA-ISP1. Esta ruta podría denotar todos los paquetes destinados a clientes de NA-ISP1. Dentro de NA-ISP1, sus routers necesitan saber a qué router de NA-ISP1 deben reenviar los paquetes de ese cliente en particular (el router denominado ISP-1 en este caso), así que las rutas situadas dentro de los routers de NA-ISP1 muestran el prefijo 2340:1111:AAAA/48.

Creación de subredes con direcciones IPv6 de unidifusión global dentro de una empresa

El diseño original de Internet con IPv4 exigía que a cada organización se le asignase un número de red con clase, y que la empresa subdividiese la red en rangos de direcciones más pequeños, creando subredes de la red con clase. Este mismo concepto de creación de subredes pasa de IPv4 a IPv6, y la empresa crea una subred del prefijo que le ha sido asignado por su ISP, empleando prefijos más pequeños. Cuando se piensa en la creación de

subredes en IPv6, se pueden establecer las siguientes analogías generales con la creación de subredes IPv4 con clase como ayuda para comprender el proceso:

- El prefijo asignado a la empresa por el ISP, que debe ser el mismo para todas las direcciones IPv6 de una misma empresa, es como la parte de red IPv4 de una dirección.
- El ingeniero de la empresa extiende la longitud del prefijo, tomando prestados bits de host, para crear la parte de subred de la dirección.
- La tercera parte importante es la parte de host de la dirección, que se denomina **ID de interfaz** en IPv6, y tiene como misión identificar de forma exclusiva a un host dentro de una subred.

Por ejemplo, la Figura 17.5 muestra una visión más detallada de la red de Empresa1 que se muestra en varias figuras anteriores de este capítulo. Los conceptos de diseño que subyacen al número de subredes necesarias en IPv6 son idénticos a los de IPv4: se necesita una subred por cada VLAN y por cada enlace serie, y las mismas opciones son válidas para subredes con Frame Relay. En este caso existen dos LANs y dos enlaces serie, así que Empresa1 precisa cuatro subredes.

La figura también muestra la forma en que el ingeniero de la empresa ha extendido la longitud del prefijo que le había asignado el ISP (/48) hasta /64, creando de este modo una parte de subred de 16 bits en la estructura de la dirección. El prefijo /48 suele llamarse **prefijo de sitio**, y el prefijo más largo que se emplea en los enlaces se denomina **prefijo de subred**. Para crear este campo de subred adicional de 16 bits, el ingeniero utiliza el mismo concepto que en IPv4 cuando se selecciona una máscara de subred tomando prestados bits del campo de host de una dirección IPv4. En este caso, piense que el campo de host tiene 80 bits (porque el prefijo asignado por el ISP tiene 48 bits de longitud, lo cual deja 80 bits) y el diseño de la Figura 17.5 toma prestados 16 bits para el campo de subred, dejando tan solo 64 bits para el campo de host.

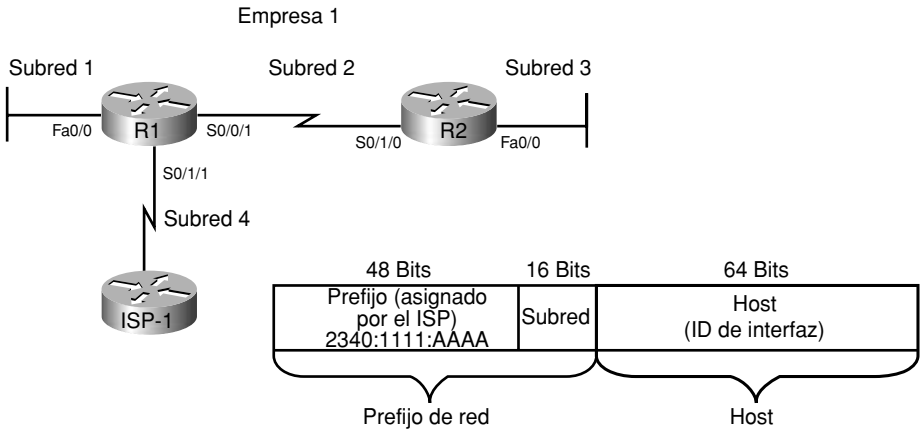


Figura 17.5. Empresa 1 necesita 4 subredes.

Un poquito de aritmética respecto a las opciones de diseño puede ofrecer una perspectiva de la escala que tiene IPv6. El campo de subred de 16 bits admite 2^{16}, o 65.536, subredes; esto es una absoluta exageración para cualquier cosa que no sean las organizaciones o compañías más enormes. (¡Tampoco hay que preocuparse por una subred cero o de difusión en IPv6!) El campo de host es, aparentemente, aún más exagerado: 2^{64} elementos por subred, que es más de 1.000.000.000.000.000.000 direcciones por subred. Sin embargo, existe una buena razón para una parte de host o de ID de interfaz tan grande, porque permite que funcione bien una de las características de asignación automática de direcciones IPv6, como se verá en la sección "Asignación de dirección de host IPv6", más adelante en este capítulo.

La Figura 17.6 lleva el concepto a su conclusión final, asignando las cuatro subredes específicas que deben utilizarse dentro de Empresa1. Obsérvese que la figura muestra los campos de subred y las longitudes de prefijo (64 en este caso) en negrita.

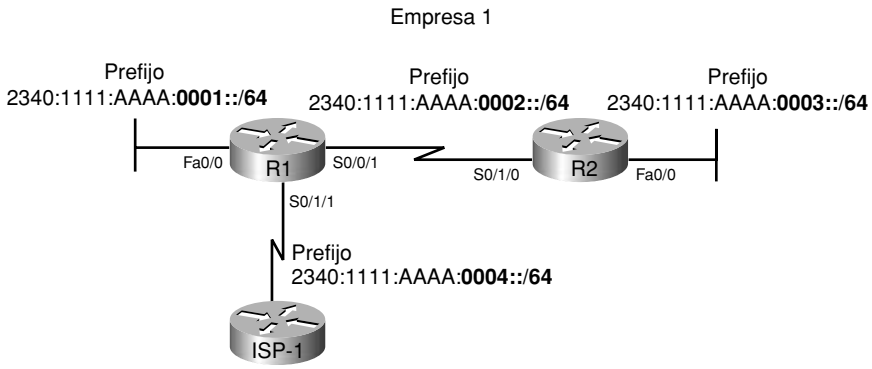


Figura 17.6. Empresa 1 con cuatro subredes asignadas.

Nota

Los números de subred de la figura se podrían abreviar ligeramente, descartando los tres ceros iniciales en los últimos cuartetos mostrados.

La Figura 17.6 sólo muestra una opción para dividir en subredes el prefijo asignado a Empresa1. Sin embargo, se podría seleccionar cualquier número de bits de subred, siempre y cuando el campo de host retuviera suficientes bits para numerar todos los hosts que hubiera en la subred. Por ejemplo, se podría emplear una longitud de prefijo /112, extendiendo el prefijo /48 por valor de 64 bits (4 cuartetos hexadecimales). Entonces, para el diseño de la Figura 17.6, se podrían seleccionar las cuatro subredes siguientes:

- 2340:1111:AAAA::0001:0000/112
- 2340:1111:AAAA::0002:0000/112

- 2340:1111:AAAA::0003:0000/112
- 2340:1111:AAAA::0004:0000/112

Al utilizar direcciones IPv6 de unidifusión globales, el enrutamiento de Internet puede ser muy eficiente y las empresas pueden tener muchas direcciones IP y muchas subredes, sin requerir funciones NAT para conservar el espacio de direcciones.

Terminología de prefijos

Antes de dar por terminado el tema, es preciso incluir unos pocos términos nuevos. El proceso de asignación de direcciones IPv6 de unidifusión globales examina muchos prefijos distintos, con muchas longitudes de prefijo diferentes. El texto muestra aquí y allá un par de términos más específicos, pero para facilitar su estudio, la Tabla 17.4 resume los cuatro términos clave, con algunos recordatorios de lo que significa cada uno.

Tabla 17.4. Ejemplos de prefijos IPv6 y de sus significados.

Término	Asignación	Ejemplo del Capítulo 17
Prefijo de registro	Otorgado por ICANN a un RIR	2340::/12
Prefijo de ISP	Otorgado por un RIR a un ISP[1]	2340:1111/32
Prefijo de sitio	Otorgado por un ISP a un cliente (sede)	2340:1111:AAAA/48
Prefijo de subred	Otorgado por un ingeniero empresarial a cada enlace individual	2340:1111:AAAA:0001/64

[1] Aunque un RIR puede asignar un prefijo a un ISP, un RIR también puede asignar un prefijo a otros registros de Internet, que pueden subdividir y asignar prefijos individuales, hasta que finalmente un ISP y sus clientes reciben algún prefijo exclusivo.

Las próximas secciones de este capítulo amplían la discusión de IPv6 para incluir tipos adicionales de direcciones IPv6, junto con los protocolos que controlan y administran varias funcionalidades comunes de IPv6.

Protocolos y direccionamiento IPv6

Los hosts IPv4 necesitan conocer varios hechos básicos antes de que puedan tener éxito en tareas sencillas, como abrir un navegador web para visualizar una página web. Normalmente, los hosts IPv4 necesitan conocer la dirección IP de uno o más servidores del servicio de nombres de dominio (DNS) para que puedan utilizar mensajes del pro-

tocolo DNS con objeto de pedir a un servidor DNS que resuelva el nombre y produzca una dirección IPv4. Necesitan conocer la dirección IP de un router que utilizarán como gateway predeterminado (el router predeterminado), para que el host que envíe paquetes a un host situado en una subred diferente los mande a ese router predeterminado. El host, por supuesto, necesita conocer su dirección IP IPv4 de unidifusión, y su máscara, o bien como se suele decir con la terminología sin clase, su dirección IPv4 y la longitud de prefijo, a partir de los cuales el host puede calcular el prefijo (la subred) de ese enlace.

Los hosts IPv6 necesitan la misma información (las direcciones IP DNS, la dirección IP del router predeterminado y su propia dirección y longitud de prefijo) por las mismas razones. Los hosts IPv6 siguen empleando nombres de host, y necesitan resolverse ese nombre en una dirección IPv6. Los hosts IPv6 siguen enviando paquetes directamente a los hosts que se encuentran en la misma subred, pero envían paquetes al router predeterminado para alcanzar destinos que están fuera de su propia subred.

Aunque los hosts IPv6 necesitan conocer la misma información, IPv6 modifica el mecanismo empleado para aprender algunos de estos datos en comparación con IPv4. Las secciones siguientes examinan las opciones y protocolos mediante los cuales los hosts pueden aprender estas informaciones clave. Al mismo tiempo, estas secciones presentan varios tipos más de direcciones IPv6 que se pueden emplear mediante los nuevos protocolos IPv6. Al final de estas secciones se resumen los detalles y la terminología de distintos tipos de direcciones IPv6.

DHCP para IPv6

Los hosts IPv6 pueden emplear el protocolo de configuración dinámica del host (*Dynamic Host Configuration Protocol*, DHCP) para detectar y aprender una dirección IP y la correspondiente longitud de prefijo (la máscara), la dirección IP del router predeterminado y la o las direcciones IP DNS. Básicamente, el concepto opera como DHCP para IPv4: el host envía un paquete IPv6 (multidifusión) en busca del servidor DHCP. Cuando responde un servidor, el cliente DHCP envía un mensaje que solicita la cesión temporal de una dirección IP, y el servidor responde con una dirección IP, una longitud de prefijo, el router predeterminado y las direcciones IP DNS. Los nombres y formatos de los mensajes DHCP en sí han cambiado bastante al pasar de IPv4 a IPv6, pero el proceso básico sigue siendo el mismo (DHCPv4 denota la versión de DHCP que se emplea para IPv4, y DHCPv6 se refiere a la versión de DHCP que se emplea para IPv6.)

Los servidores DHCPv4 retienen información relativa a cada cliente, como la dirección IP cedida a ese cliente y la cantidad de tiempo durante la cual es válida la cesión. Este tipo de información se denomina **información de estado**, porque realiza un seguimiento del estado de cada cliente. Los servidores DHCPv6, a su vez, poseen dos modos de operación: con estado, en el cual el servidor rastrea la información de estado, y el modo sin estado, en el cual el servidor no hace un seguimiento de la información de estado. Los servidores DHCPv6 con estado desempeñan el mismo papel que los viejos servidores DHCPv4,

mientras que los servidores DHCPv6 sin estado desempeñan un papel perteneciente a una alternativa IPv6 del DHCP con estado. (El DHCP sin estado, y su propósito, se trata en la siguiente sección.)

Una diferencia entre DHCPv4 y DHCPv6 con estado es que los hosts IPv4 envían difusiones IP para buscar servidores DHCP, mientras que hosts IPv6 envían multidifusiones IPv6. Las direcciones multidifusión IPv6 tienen el prefijo FF00::/8, lo cual significa que los ocho primeros bits de la dirección son 11111111 en binario, o FF en hexadecimal. La dirección de multidifusión FF02::1:2 (o en su versión no abreviada, FF02:0000:0000:0000:0000:0000:0001:0002) se ha reservado en IPv6 para que la utilicen los hosts con objeto de enviar paquetes a un servidor DHCP desconocido, y los routers reenvían estos paquetes al servidor DHCP correspondiente.

Asignación de dirección de host IPv6

Cuando se utiliza IPv4 en redes empresariales, los ingenieros normalmente configuran direcciones IPv4 estáticas en las interfaces de todos los routers, empleando el subcomando de interfaz `ip address`. Al mismo tiempo, muchos hosts de usuarios finales emplean DHCP para aprender dinámicamente su dirección IP y su máscara. Para acceder a Internet, el router puede utilizar DHCP para aprender su propia dirección pública IPv4 del ISP.

IPv6 sigue el mismo modelo en general, pero los routers emplean uno de entre dos procesos para la asignación de direcciones IPv6 estática, y los hosts de los usuarios finales emplean una de entre dos opciones para la asignación de direcciones IPv6 dinámicas. Las secciones siguientes examinan las cuatro opciones. Pero en primer lugar, para poder apreciar las opciones de configuración, se necesita un poco más de información sobre los 64 bits inferiores del formato de la dirección de IPv6: el ID de interfaz.

El ID de interfaz IPv6 y el formato EUI-64

En una parte anterior de este capítulo la Figura 17.5 muestra el formato de una dirección de unidifusión global IPv6, en la que la segunda mitad de la dirección se denomina ID de host o de interfaz. El valor de la parte de ID de interfaz en una dirección unidifusión global puede recibir cualquier valor, siempre y cuando no haya otro host de la misma subred que intente emplear ese mismo valor. (IPv6 incluye un método dinámico para que hosts averigüen si existe una dirección duplicada en la subred antes de empezar a utilizar la dirección). Sin embargo, el tamaño del ID de interfaz se ha seleccionado deliberadamente para permitir una configuración sencilla de las direcciones IP, insertando la dirección MAC de una tarjeta de red en el campo de ID de interfaz de una dirección IPv6.

Las direcciones MAC tienen 6 bytes (48 bits) de longitud, así que para que un host decida automáticamente el valor que debe utilizar en el campo de ID de interfaz de 8 bytes, IPv6 no

puede limitarse a copiar la dirección MAC. Para completar la interfaz de 64 bits, IPv6 rellena dos bytes más. Curiosamente, para hacer esto, IPv6 separa la dirección MAC en dos mitades de 3 bytes, e inserta el número hexadecimal FFFE entre ambas mitades, para así formar el campo de ID de interfaz, y también para dar el valor binario 1 a un bit especial.

Este formato, que se denomina formato EUI-64, se muestra en la Figura 17.7.

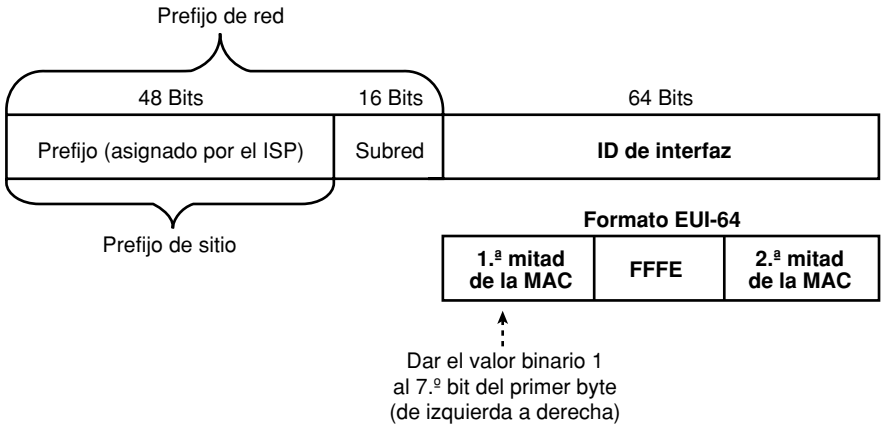


Figura 17.7. Formato de la dirección IPv6 con ID de interfaz y EUI-64.

Aunque pueda parecer un poquito barroco, funciona. Además, con un poco de práctica, se puede examinar una dirección IPv6 y se observa rápidamente el FFFE que hay al final de la dirección, para después hallar fácilmente las dos mitades de la correspondiente dirección MAC de la interfaz.

Para completar, la figura señala otro detallito relativo al valor del ID de interfaz EUI-64. Partir en dos mitades la dirección MAC e insertar el valor FFFE resulta sencillo. Sin embargo, el formato EUI-64 exige que el séptimo bit del primer byte del valor sea un 1 binario. La razón subyacente es que las direcciones MAC de Ethernet se muestran con los bits menos significativos de cada byte a la izquierda, y los bits más significativos a la derecha. Por tanto, el octavo bit de un byte (leyendo de izquierda a derecha) es el bit más significativo de la dirección, y el séptimo bit (leyendo de izquierda a derecha) es el segundo bit más significativo. Este segundo bit más significativo del primer byte (que es el séptimo bit de izquierda a derecha) recibe el nombre de bit universal/local (U/L). Si se le da el valor 0, significa que es una dirección MAC inamovible. Si se le asigna el valor 1, significa que la dirección MAC ha sido configurada localmente. EUI-64 dice que el bit U/L debe tener el valor 1, para indicar que es local.

Por ejemplo, las dos líneas siguientes muestran la dirección MAC de un host y el correspondiente ID de interfaz en formato EUI-64, suponiendo que se utilizase una opción de configuración de dirección que hiciera uso del formato EUI64:

- 0034:5678:9ABC
- 0234:56FF:FE78:9ABC

NOTA

Para modificar el séptimo bit (leyendo de izquierda a derecha) en el ejemplo, se convierte el 00 hexadecimal en el binario 00000000, se cambia el séptimo bit por un 1 (00000010), y después se vuelve a convertir a hexadecimal, que es 02 en hexadecimal para los dos primeros dígitos.

Configuración estática de direcciones IPv6

En este libro se tratan dos opciones de configuración de direcciones IPv6 estáticas, y ambas están disponibles tanto en routers como en hosts: la configuración estática de toda la dirección y la configuración estática de un prefijo /64 haciendo que la computadora calcule su ID de interfaz EUI-64 para completar la dirección IP. Esta sección ilustra el concepto empleando routers.

Para configurar una dirección IPv6 en una interfaz, el router necesita un subcomando de interfaz ipv6 address *dirección/longitud-de-prefijo* [eui-64] en cada interfaz. Si no se incluye la palabra reservada eui-64, la dirección debe representar toda la dirección entera de 128 bits. Si se incluye la palabra reservada eui-64, la dirección debería representar el prefijo de 64 bits, y el router creará el ID de interfaz empleando el formato EUI-64. EL parámetro *longitud-de-prefijo* debería ser la longitud del prefijo de subred. Por ejemplo, el Ejemplo 17.1 muestra los comandos del router R1 visto anteriormente en la Figura 17.6, que es uno de los routers de la empresa Empresa1. Utiliza una longitud de prefijo de sitio igual a /64. El ejemplo muestra ambas versiones del comando (con y sin la palabra reservada eui-64).

Ejemplo 17.1. Configuración estática de direcciones IPv6.

```
! La primera interfaz está en la subred 1, y utilizará EUI-64 como ID de Interfaz
!
interface FastEthernet0/0
 ipv6 address 2340:1111:AAAA:1::/64 eui-64
! La interfaz siguiente indica los 128 bits, abreviando. La versión larga es
! 2340:1111:AAAA:0003:0000:0000:0001/64. Se halla en la subred 2.
!
interface Serial0/0/1
 ipv6 address 2340:1111:AAAA:2::1/64
! La tercera interfaz está en la subred 4, también con ID de interfaz
! en formato EUI-64.
!
interface Serial0/1/1
 ipv6 address 2340:1111:AAAA:4::/64 eui-64
!
R1#show ipv6 interface fa0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::213:19FF:FE7B:5004
```

(continúa)

Ejemplo 17.1. Configuración estática de direcciones IPv6 *(continuación).*

```
  Global unicast address(es):
    2340:1111:AAAA:1:213:19FF:FE7B:5004, subnet is 2340:1111:AAAA:1::/64 [EUI]
! Se han omitido ciertas líneas por brevedad
R1#show ipv6 interface S0/0/1
Serial0/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::213:19FF:FE7B:5004
  Global unicast address(es):
    2340:1111:AAAA:3::1, subnet is 2340:1111:AAAA:3::/64
! Se han omitido ciertas líneas por brevedad
R1#show ipv6 interface s0/1/1
Serial0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::213:19FF:FE7B:5004
  Global unicast address(es):
    2340:1111:AAAA:4:213:19FF:FE7B:5004, subnet is 2340:1111:AAAA:4::/64 [EUI]
! Se han omitido ciertas líneas por brevedad
```

El final del ejemplo muestra la dirección IPv6 de unidifusión global completa como parte del comando show ipv6 interface. Cuando se utiliza la opción EUI-64, este comando resulta especialmente útil, porque el comando de configuración no muestra la dirección IPv6 completa. Obsérvese que si se utiliza el formato EUI, entonces el comando show ipv6 interface tiene en cuenta ese hecho (véanse las interfaces Fa0/0 y S0/1/1, frente a S0/0/1). Además, los routers no tienen direcciones MAC asociadas a determinadas interfaces, incluyendo las interfaces serie, así que para formar el ID de interfaz con formato EUI-64 en esas interfaces, los routers emplean la dirección MAC de una interfaz LAN. En este caso, el ID de interfaz de S0/1/1 está basado en la dirección MAC de Fa0/0.

Autoconfiguración sin estado y publicaciones de los routers

IPv6 admite dos métodos de configuración dinámica de direcciones IPv6. Uno hace uso de un servidor DHCPv6 con estado que, como se mencionaba anteriormente, funciona conceptualmente igual que DHCP en IPv4, aunque entre DHCPv4 y DHCPv6 difieren muchos detalles de los mensajes. IPv6 ofrece también una alternativa denominada **autoconfiguración sin estado** (que no debe confundirse con DHCP sin estado, que se trata en esta sección). Al emplear la autoconfiguración sin estado, el host aprende dinámicamente el prefijo /64 utilizado en la subred, y después calcula el resto de su dirección empleando un ID de interfaz EUI-64 basado en la dirección MAC de su tarjeta de interfaz de red (NIC).

El proceso de autoconfiguración hace uso de una de las muchas características del Protocolo de descubrimiento de vecindad (NDP) de IPv6 para descubrir el prefijo utilizado en la LAN. NDP desempeña muchas funciones en IPv6, y todas ellas están relacionadas con algo que sucede entre dos hosts de la misma subred. Por ejemplo, una parte

de NDP reemplaza al protocolo ARP de IPv4. El ARP de IPv4 permite a dispositivos de la misma subred (los vecinos) conocer la dirección MAC de los otros vecinos. Como esta actividad y muchas otras suceden solamente dentro de la subred local entre vecinos del mismo enlace, IPv6 ha reunido todas estas funciones básicas en un conjunto de protocolos denominado NDP.

La autoconfiguración sin estado utiliza dos mensajes NDP, a saber, la solicitud de router (RS) y la publicación de router (RA) con objeto de descubrir el prefijo IPv6 que se está utilizando en la LAN. El host envía el mensaje RS en forma de un mensaje de multidifusión IPv6, pidiendo a todos los routers que respondan a las preguntas "¿Qué prefijo o prefijos IPv6 se utilizan en esta subred?" y "¿Cuáles son las direcciones IPv6 de los routers predeterminados de esta subred?" La Figura 17.8 muestra la idea general, en la subred 1 de la Figura 17.3, en donde PC1 envía un RS, y el router R1 responde con el prefijo IPv6 que se utiliza en la LAN, y con la dirección IPv6 del propio R1 como router predeterminado potencial.

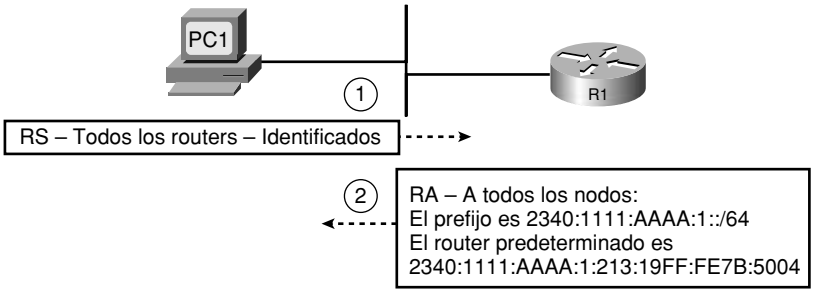


Figura 17.8. Ejemplo del proceso NDP RS/RA para buscar los routers predeterminados.

Nota

IPv6 permite enumerar múltiples prefijos y múltiples routers predeterminados en el mensaje RA; la figura sólo muestra uno de cada clase por sencillez.

IPv6 no utiliza difusiones. De hecho, no existe tal cosa como una dirección de difusión de subred, una dirección de difusión a toda la red, o una equivalente de la dirección IPv4 de difusión a todos los hosts, 255.255.255.255. En su lugar, IPv6 utiliza direcciones de multidifusión. Al usar una dirección IPv6 de multidifusión distinta para distintas funciones, si un host no tiene necesidad de participar en una determinada acción, puede muy bien ignorar esas multidifusiones en particular, reduciendo el impacto sobre ese host. Por ejemplo, el mensaje RS sólo tiene que ser recibido y procesado por los routers, así la dirección IP de destino del mensaje RS es FF02::2, que es la dirección reservada en IPv6 para ser utilizada únicamente por routers IPv6. Los mensajes RA se envían a una dirección de multidifusión destinada a ser empleada por todos los hosts IPv6 que haya en el enlace (FF02::1), así que no sólo aprenderá la información

el host que haya enviado el RS, sino que además todos los demás hosts que haya en el enlace recibirán los detalles.

La Tabla 17.5 resume algunos de los detalles clave relativos a los mensajes RS/RA.

Tabla 17.5. Detalles del proceso RS/RA.

Mensaje	**RS**	**RA**
Destino multidifusión	FF02::2	FF02::1
Significado de la dirección de multidifusión	Todos los routers de este enlace	Todos los nodos IPv6 de este enlace

Resumen de la configuración de direcciones en IPv6

Este capítulo trata cuatro métodos destinados a asignar direcciones IPv6 a hosts o a interfaces de un router. Hay dos variantes que emplean una configuración estática, y otras dos que aprenden dinámicamente la dirección. Sin embargo, tanto en las configuraciones estáticas como en las dinámicas, hay dos alternativas: una que aporta toda la dirección IPv6 y otra que permite al host calcular el ID de interfaz EUI-64. La Tabla 17.6 resume los métodos de configuración.

Tabla 17.6. Opciones de configuración de IPv6.

Estática o dinámica	**Opción**	**Porción configurada o aprendida**
Estática	No utilizar EUI-64	Toda la dirección de 128 bits
Estática	Utilizar EUI-64	Solamente el prefijo /64
Dinámica	DHCPv6 con estado	Toda la dirección de 128 bits
Dinámica	Autoconfiguración con estado	Solamente el prefijo /64

Descubrimiento del router predeterminado mediante NDP

En IPv4, los hosts descubren su router predeterminado (el gateway predeterminado) bien mediante configuración estática en el host o, más normalmente, mediante DHCP. IPv6 puede utilizar también estas dos opciones, así como los mensajes NDP RS/RA descritos en la sección anterior. El proceso de descubrimiento de router de NDP se produce de forma predeterminada en los host y routers IPv6, así que aunque el servidor DHCPv6 con

estado puede proporcionar la dirección o direcciones IP de los posibles routers predeterminados, es perfectamente razonable en IPv6 no molestarse en configurar estos detalles en un servidor DCHP con estado, permitiendo que los mensajes de NDP RS/RA se utilicen en su lugar.

El proceso de descubrimiento del router predeterminado es relativamente sencillo. Los routers envían automáticamente mensajes RA de forma periódica. Estos mensajes no sólo muestran la dirección IPv6 del router remitente, sino también la de todos los routers conocidos en esa subred. Los hosts pueden esperar al próximo mensaje RA periódico, o pueden solicitar que todos los routers locales envíen un RA inmediatamente, pidiéndoselo a todos los routers mediante el mensaje RS.

Aprendizaje de la dirección o direcciones IP de los servidores DNS

Al igual que los hosts IPv4, los hosts IPv6 necesitan normalmente conocer la dirección IP de uno o más servidores DNS para resolver lo nombres y obtener la correspondientes dirección IP. Con frecuencia, el elemento también necesita aprender el nombre de dominio DNS que debe utilizar. Y al igual que en los hosts IPv4, los hosts IPv6 pueden recibir estas direcciones IP empleando DHCP (con estado). Cuando un host (o un router, a decir verdad) obtiene su dirección IPv6 empleando DHCP con estado, ese host también puede obtener las direcciones IP del servidor DNS y el nombre del dominio, resolviendo así esta cuestión.

El DHCP sin estado, que resulta especialmente útil en conjunción con la autoconfiguración sin estado, es un método alternativo para obtener las direcciones IP del servidor DNS y el nombre del dominio. Cuando un elemento utiliza la autoconfiguración sin estado, puede obtener su dirección IPv6 y su prefijo automáticamente, y también puede aprender la dirección IP de su router predeterminado, empleando en ambos casos mensajes NDP RS/RA. Sin embargo, el proceso de autoconfiguración sin estado no ayuda al host a determinar las direcciones IP DNS, ni el nombre del dominio. Por tanto, el DHCP sin estado aporta esa información empleando los mismos mensajes que el DHCP con estado. Sin embargo, para aportar esta información, el servidor no necesita rastrear ninguna información de estado de los clientes, así que se puede emplear un servidor DHCP sin estado.

La Tabla 17.7 resume algunas de las características clave de DHCPv6 con y sin estado.

Direcciones IPv6

Este capítulo ya ha presentado los conceptos que subyacen al formato general de las direcciones IPv6, las ideas que subyacen a las direcciones IPv6 de unidifusión global, y algunos detalles relativos a las direcciones IPv6 de multidifusión. Las secciones siguientes

Tabla 17.7. Comparación de los servicios DHCPv6 con estado y sin estado.

Características	DHCP con estado	DHCP sin estado
Recuerda las direcciones IPv6 (la información de estado) de aquellos clientes que piden solicitudes	Sí	No
Asigna una dirección IPv6 al cliente	Sí	No
Aporta información útil, como las direcciones IP de servidores DNS	Sí	Sí
De especial utilidad si se usa junto con una autoconfiguración sin estado	No	Sí

completan nuestros conocimientos del direccionamiento, y más específicamente lo relativo a las tres categorías de direcciones IPv6:

- **Unidifusión:** Se asignan direcciones IP a una sola interfaz con el propósito de permitir que un host envíe y reciba datos.
- **Multidifusión:** Direcciones IP que representan un grupo dinámico de hosts con el propósito de enviar paquetes a todos los miembros actuales del grupo. Algunas direcciones de multidifusión se emplean con propósitos especiales, como en el caso de los mensajes NDP, aunque la mayoría se utiliza para aplicaciones de usuario final.
- **Tododifusión (*anycast*):** Es una opción de diseño mediante la cual los servidores que admiten una misma función pueden utilizar la misma dirección IP de unidifusión, y los paquetes que envían los clientes se reenvían al servidor más cercano, lo cual permite equilibrar la carga entre distintos servidores.

Direcciones IPv6 de unidifusión

IPv6 admite tres clases principales de direcciones de unidifusión. Una de estas clases, las direcciones IP de unidifusión globales, se asemeja mucho al propósito de las direcciones IP públicas de IPv4. Las direcciones de unidifusión global son asignadas por ICANN y los RIRs con el propósito de permitir direcciones IPv6 exclusivas globalmente para todos los hosts. Estas direcciones provienen del interior del prefijo 2000::/3, que incluye todas las direcciones que comienzan por 2 ó 3 (en hexadecimal).

La siguiente clase de direcciones de unidifusión IPv6 que se trata aquí, las direcciones de unidifusión **locales exclusivas**, tienen la misma función que las direcciones privadas de IPv4 descritas en la RFC 1918. En IPv4, casi todas las empresas, y casi todas las oficinas pequeñas o domésticas, utilizan redes privadas IPv4. Las direcciones de unidifusión **locales exclusivas** comienzan por FD en hexadecimal (FD00::/8), y tienen el formato que se muestra en la Figura 17.9.

NOTA

Las RFCs originales de IPv6 definían una clase de dirección privada llamada local de sitio, que denotaba una dirección local dentro de un sitio (una organización). La clase de direcciones locales de sitio ha sido desaconsejada, y se ha sustituido por direcciones de unidifusión locales exclusivas.

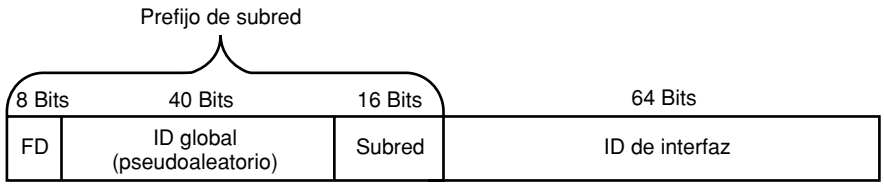


Figura 17.9. Formato de una dirección local exclusiva.

Para utilizar estas direcciones, los ingenieros de empresa utilizarían un ID global de 40 bits de forma pseudoaleatoria, con la intención de que las direcciones sean realmente exclusivas en el universo. En realidad, pseudoaleatorio se refiere probablemente a un número que ha inventado el ingeniero. El campo de subred de 16 bits y el ID de interfaz de 64 bits se comportan igual que con las direcciones de unidifusión globales, dando números a las distintas subredes y elementos, y permitiendo dar valores EUI-64 al ID de interfaz. Como de costumbre, el ingeniero podría evitar utilizar EUI-64, empleando valores más fáciles de recordar como 0000:0000:0000:0001 para el ID de interfaz.

Las direcciones locales de enlace son la tercera clase de direcciones IPv6 de unidifusión que se trata aquí. IPv4 no tiene conceptos como el de dirección IP local de enlace. IPv6 emplea estas direcciones cuando envía paquetes a través de la subred local; los routers nunca reenvían a otras subredes los paquetes destinados a direcciones locales de enlace.

Las direcciones locales de enlace pueden ser útiles para aquellas funciones que no necesitan abandonar la subred, en particular porque un host puede derivar automáticamente su propia dirección IP local de enlace sin enviar paquetes a través de la subred. Por tanto, antes de enviar los primeros paquetes, el host puede calcular su propia dirección local de enlace para que tenga una dirección IPv6 que pueda usar cuando envíe sus primeros mensajes adicionales. Por ejemplo, antes de que un host envíe un mensaje NDP RS (de solicitud de router), el host ya habrá calculado su dirección local de enlace. El host utiliza su dirección local de enlace como dirección IP de origen en el mensaje RS.

Las direcciones locales de enlace provienen del rango FE80::/10, lo cual significa que todas esas direcciones empiezan por FE80, FE90, FEA0 y FEB0. No se requiere una configuración específica, porque un host forma esas direcciones empleando los diez primeros bits del número hexadecimal FE80 (que es 1111111010 en binario), 54 ceros binarios adicionales, y los últimos 64 bits que son el ID de interfaz del host, con formato EUI-64. La Figura 17.10 muestra el formato.

10 Bits	54 Bits	64 Bits
FE80/10 1111111010	Todo ceros	ID de interfaz

Figura 17.10. Formato de la dirección local de enlace.

Los routers también emplean direcciones locales de enlace en todas las interfaces que están habilitadas par admitir IPv6. Al igual que los hosts, los routers calculan automáticamente sus direcciones IP locales de enlace. De hecho, en el Ejemplo 17.1 visto anteriormente en este capítulo, se mostraban las direcciones IP locales del router R1 en la salida del comando `show ipv6 interface`. Curiosamente, los routers suelen utilizar direcciones locales de enlace como dirección IP de siguiente salto en las rutas IPv6, en lugar de emplear la dirección de unidifusión global o la dirección de unidifusión local exclusiva del router vecino.

Multidifusión y otras direcciones IPv6 especiales

Las direcciones de multidifusión se pueden emplear para comunicarse con agrupaciones dinámicas de hosts, de tal modo que el remitente envía un único paquete y la red duplica el paquete según sea necesario para que todos los hosts que estén a la escucha de paquetes enviados a esa dirección de multidifusión reciban una copia del paquete. IPv6 puede limitar el alcance dentro del cual los routers reenvían multidifusiones, basándose en el valor del primer cuarteto de la dirección. Este libro sólo examina las multidifusiones que deben permanecer en un enlace local; todas estas direcciones comienzan por FF02::/16, así que se reconocen fácilmente.

Como referencia, la Tabla 17.8 muestra algunas de las direcciones de multidifusión que se ven más frecuentemente en IPv6. Resultan de especial interés las direcciones seleccionadas para su uso en el Protocolo de información de enrutamiento (RIP), en Primero la ruta libre más corta (OSPF), y en el IGRP mejorado (EIGRP), que hasta cierto punto se asemejan a las direcciones de multidifusión que utilizan los mismos protocolos en IPv4.

Antes de terminar la descripción del direccionamiento IPv6, hay que conocer un par de direcciones IPv6 especiales. En primer lugar, IPv6 admite el concepto de dirección IP de *loopback*, en la forma siguiente:

::1 (127 ceros binarios y un 1)

Exactamente igual que la dirección de *loopback* 127.0.0.1 que hay en IPv4, esta dirección se puede emplear para probar el software de un host. Los paquetes enviados por un host a esta dirección bajan por la pila del protocolo y vuelven a subir, sin establecer comunicación con la tarjeta de red subyacente. Esto permite comprobar el software en el host, sobre todo cuando se prueban nuevas aplicaciones.

La otra dirección especial es la dirección :: (todo son ceros binarios). Esta dirección representa la dirección desconocida, que puede ser utilizada por los hosts cuando envían paquetes intentando descubrir sus propias direcciones IP.

Tabla 17.8. Direcciones de multidifusión de enlace local más frecuentes.

Propósito	Dirección IPv6	Equivalente IPv4
Todos los nodos IP del enlace	FF02::1	Dirección de difusión en la subred
Todos los routers del enlace	FF02::2	No existe
Mensajes OSPF	FF02::5, FF02::6	224.0.0.5, 224.0.0.6
Mensajes RIP-2	FF02::9	224.0.0.9
Mensajes EIGRP	FF02::A	224.0.0.10
Agentes relay para DHCP (routers que envían hacia el servidor DHCP)	FF02:1:2	No existe

Resumen de los protocolos y el direccionamiento IP

Este capítulo ha tratado muchos conceptos y muchos detalles relativos a las direcciones IPv6, y todo esto requiere un cierto esfuerzo para recordarlo o memorizarlo. Esta breve sección reúne varios conceptos de toda la sección principal dedicada a los protocolos y las direcciones IPv6, antes de pasar a exponer ciertos detalles de los protocolos de enrutamiento y de la configuración de routers.

Cuando arranca un host IPv6 por primera vez, necesita realizar varias tareas antes de que le sea posible enviar paquetes a otro host a través de un router. Cuando se utiliza uno de los dos métodos para aprender dinámicamente la dirección IPv6 que se puede emplear para enviar paquetes a través de los routers locales hacia el resto de la red, los primeros pasos de iniciación son los mismos, con algunas diferencias en los pasos posteriores. La lista siguiente resume los pasos que da un host cuando arranca por primera vez, al menos para las funciones tratadas en este capítulo:

Paso 1 El host calcula su dirección local de enlace IPv6 (comienza por FE80::/10).

Paso 2 El host envía un mensaje de solicitud de router NDP (un RS), con su dirección local de enlace como dirección de origen y la dirección de destino de multidifusión FF02::2 para todos los routers, con objeto de pedir a los routers que aporten una lista de routers predeterminados y el prefijo/longitud que se emplea en la LAN.

Paso 3 El router o routers responden con un mensaje RA, enviado desde la dirección local de enlace del router, y remitido a la dirección de multidifusión que deno-

ta todos los hosts IPv6 del enlace (FF02::1), aportando la información de router predeterminado y de prefijo.

Paso 4 Si el tipo de asignación de dirección dinámica es una autoconfiguración sin estado, ocurre lo siguiente:

a. El host construye la dirección IP de unidifusión que puede emplear para enviar paquetes a través del router, utilizando el prefijo que ha aprendido en el mensaje RA y calculando un ID de interfaz EUI-64 basado en la dirección MAC de la tarjeta de red.

b. El host emplea mensajes DHCP para pedir a un servidor DHCP sin estado las direcciones IP del servidor DNS y el nombre del dominio.

Paso 4 Si el tipo de asignación dinámica de direcciones es DHCP con estado, el host utiliza mensajes DHCP para pedir a un servidor DHCP con estado el alquiler de una dirección IP y una longitud de prefijo, así como las direcciones de router predeterminado, las direcciones IP del servidor DNS y el nombre del dominio.

Nota

Hay otras tareas que ocurren cuando arranca el host, pero van más allá del alcance de este libro.

IPv6 incluye muchos tipos de direcciones diferentes, incluyendo de unidifusión y de multidifusión. A modo de resumen, la Tabla 17.9 enumera los tipos de direcciones IPv6 que se han mencionado en este capítulo con algunos detalles, para que sirvan como referencia sencilla para su estudio.

Tabla 17.9. Direcciones comunes de multidifusión local de enlace.

Tipo de dirección	Propósito	Prefijo	Prefijo o prefijos hexadecimales fáciles de detectar
Unidifusión global	Paquetes de unidifusión enviados a través de la Internet pública	2000::/3	2 ó 3
Local exclusiva	Paquetes de unidifusión dentro de una organización	FD00::/8	FD
Local de enlace	Paquetes enviados en la subred local	FE80::/10	FE8, FE9, FEA, FEB
Multidifusión (alcance local de enlace)	Multidifusiones que permanecen en la subred local	FF02::/16	FF02

Configuración del enrutamiento y de los protocolos de enrutamiento en IPv6

Para admitir IPv6, todos los protocolos de enrutamiento IPv4 tenían que pasar por cambios en mayor o menor grado, y el más evidente era que todo tenía que cambiar para admitir direcciones y prefijos más largos. Las secciones siguientes examinan primero algunos detalles relativos a los protocolos de enrutamiento y después muestran la forma de configurar el enrutamiento en IPv6 y los protocolos de enrutamiento que ofrecen los routers de Cisco.

Protocolos de enrutamiento IPv6

Tal como sucedía con IPv4, la mayoría de los protocolos de enrutamiento de IPv6 son protocolos de gateway interno (IGP), y el Protocolo de gateway fronterizo (BGP) sigue siendo el único protocolo de gateway exterior (EGP) que tiene alguna importancia. Todos estos IGPs y BGPs actuales se han actualizado para admitir IPv6. La Tabla 17.10 muestra los protocolos de enrutamiento y sus nuevas RFCs (según conviene).

Tabla 17.10. Actualizaciones de los protocolos de enrutamiento para IPv6.

Protocolo de enrutamiento	Nombre completo	RFC
RIPng	RIP de nueva generación	2080
OSPFv3	OSPF versión 3	2740
MP-BGP4	BGP-4 multiprotocolo	2545/4760
EIGRP para IPv6	EIGRP para IPv6	Privado

Cada uno de estos protocolos de enrutamiento tiene que experimentar varios cambios para admitir IPv6. Los mensajes que se emplean para enviar y recibir información de enrutamiento han cambiado, y emplean encabezados de IPv6 en lugar de encabezados de IPv4, y utilizan direcciones IPv6 en esos encabezados. Por ejemplo, RIPng envía paquetes de enrutamiento a la dirección IPv6 de destino FF02::9, en lugar de emplear la antigua dirección RIP-2 de IPv4 que era 224.0.0.9. Además, los protocolos de enrutamiento típicamente publican su dirección IP local de enlace como siguiente salto dentro de una ruta, como se verá en el Ejemplo 17.2.

Los protocolos de enrutamiento siguen reteniendo muchas de las mismas características internas. Por ejemplo, RIPng, al estar basado en RIP-2, sigue siendo un protocolo por vector de distancia, con el número de saltos como métrica y 15 saltos como ruta válida más larga (16 es infinito). OSPFv3, creado específicamente para soportar IPv6,

sigue siendo un protocolo por estado del enlace, con el coste como métrica pero con muchas características internas cambiadas, incluyendo los tipos de publicación de estado del enlace (LSA). Como resultado, OSPFv2, tal como se describe en el Capítulo 9, "OSPF", no es compatible con OSPFv3. Sin embargo, los conceptos operativos básicos siguen siendo los mismos.

Configuración de IPv6

El IOS de los routers de Cisco habilita el enrutamiento (envío) de paquetes IPv4 de forma predeterminada, e IPv4 se habilita en las interfaces cuando esas interfaces tienen configurada una dirección IPv4. Para los protocolos de enrutamiento IPv4, el protocolo de enrutamiento tiene que ser configurado, y el comando `network` habilita indirectamente el protocolo de enrutamiento en la interfaz.

La configuración de IPv6 sigue algunas de estas líneas generales, y la diferencia más importante es la forma de habilitar un protocolo de enrutamiento en una interfaz. El IOS de los routers de Cisco no habilita el enrutamiento IPv6 de forma predeterminada, así que se necesita un comando global para activarlo. Las direcciones IP de unidifusión tienen que estar configuradas en las interfaces, de forma similar a IPv4. El protocolo de enrutamiento tiene que estar configurado globalmente, de forma similar a IPv4. Por último, el protocolo de enrutamiento tiene que ser configurado en cada interfaz a medida que es necesario, pero en IPv6 el proceso no utiliza el subcomando de router `network`.

Esta sección muestra un ejemplo de configuración, que una vez más hace uso del Router R1 de la red de Empresa1 utilizado en las figuras anteriores del capítulo. El ejemplo hace uso de RIPng como protocolo de enrutamiento. La lista siguiente muestra los cuatro pasos principales que deben darse para configurar IPv6:

Paso 1 Activar el enrutamiento IPv6 usando el comando global `ipv6 unicast-routing`.

Paso 2 Activar el protocolo de enrutamiento seleccionado. Por ejemplo, para RIPng, utilizar el comando de configuración global `ipv6 router rip` *nombre*.

Paso 3 Configurar una dirección de unidifusión IPv6 en cada interfaz, empleando el comando de interfaz `ipv6 address` *dirección/longitud-prefijo* `[eui-64]`.

Paso 4 Activar el protocolo de enrutamiento en la interfaz, por ejemplo mediante el subcomando de interfaz `ipv6 rip` *nombre* `enable` (donde el nombre coincide con el dado en el comando de configuración global `ipv6 router rip` *nombre*).

El Ejemplo 17.2 muestra la configuración, más unos pocos comandos `show`. Obsérvese que la configuración de la dirección IP coincide con el Ejemplo 17.1 visto anteriormente. Como el Ejemplo 17.1 mostraba la configuración de la dirección, este ejemplo muestra resaltados sólo los nuevos comandos de configuración.

La configuración en sí no requiere mucho trabajo más allá de la configuración de la dirección IPv6 que se ha mostrado previamente en el Ejemplo 17.1. El comando `ipv6 router rip` *nombre* requiere un nombre (que formalmente se denomina etiqueta) que no es otra cosa que un nombre en formato de texto para el proceso de enrutamiento. El Ejemplo 17.2 muestra la configuración, empleando una etiqueta RIP denominada

Ejemplo 17.2. Configuración del enrutamiento IPv6 y de sus protocolos de enrutamiento en R1.

```
R1#show running-config
! Se ha modificado la salida para eliminar líneas que no son pertinentes para este
! ejemplo
ipv6 unicast-routing
!
interface FastEthernet0/0
 ipv6 address 2340:1111:AAAA:1::/64 eui-64
 ipv6 rip atag enable
!
interface Serial0/0/1
 ipv6 address 2340:1111:AAAA:2::1/64
 ipv6 rip atag enable
!
interface Serial0/1/1
 ipv6 address 2340:1111:AAAA:4::/64 eui-64
 ipv6 rip atag enable
!
ipv6 router rip atag
!
R1#show ipv6 route
IPv6 Routing Table - 10 entries
Codes:  C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R ::/0 [120/2]
         via FE80::213:19FF:FE7B:2F58, Serial0/1/1
C       2340:1111:AAAA:1::/64 [0/0]
         via ::, FastEthernet0/0
L       2340:1111:AAAA:1:213:19FF:FE7B:5004/128 [0/0]
         via ::, FastEthernet0/0
C       2340:1111:AAAA:2::/64 [0/0]
         via ::, Serial0/0/1
L       2340:1111:AAAA:2::1/128 [0/0]
         via ::, Serial0/0/1
R       2340:1111:AAAA:3::/64 [120/2]
         via FE80::213:19FF:FE7B:5026, Serial0/0/1
C       2340:1111:AAAA:4::/64 [0/0]
         via ::, Serial0/1/1
L       2340:1111:AAAA:4:213:19FF:FE7B:5004/128 [0/0]
         via ::, Serial0/1/1
L       FE80::/10 [0/0]
         via ::, Null0
L       FF00::/8 [0/0]
         via ::, Null0
```

(continúa)

Ejemplo 17.2. Configuración del enrutamiento IPv6 y de sus protocolos de enrutamiento en R1 *(continuación).*

```
R1#show ipv6 interface brief
FastEthernet0/0             [up/up]
    FE80::213:19FF:FE7B:5004
    2340:1111:AAAA:1:213:19FF:FE7B:5004
FastEthernet0/1             [up/up]
    unassigned
Serial0/0/0                 [administratively down/down]
    unassigned
Serial0/0/1                 [up/up]
    FE80::213:19FF:FE7B:5004
    2340:1111:AAAA:2::1
Serial0/1/0                 [administratively down/down]
    unassigned
Serial0/1/1                 [up/up]
    FE80::213:19FF:FE7B:5004
    2340:1111:AAAA:4:213:19FF:FE7B:5004
```

"atag". Esta etiqueta no tiene por qué coincidir entre los distintos routers. Al margen de esto, la configuración en sí es más bien sencilla.

El comando show ipv6 route muestra todas las rutas de IPv6, indicando algunas diferencias importantes, que se han resaltado en la salida del comando. En primer lugar, observe las primeras líneas resaltadas, y el nuevo código de enrutamiento "L". Para toda interfaz que tenga una dirección de unidifusión, el router añade la ruta conectada habitual para el prefijo conectado a esa interfaz. Por ejemplo, la primera línea resaltada en este comando muestra 2340:1111:AAAA:1::/64, que es la subred conectada a la interfaz Fa0/0 de R1. El router también muestra una ruta de host (una ruta con el prefijo de longitud /128) como ruta local. Todas estas rutas locales, según se indica con el código "L", muestran la dirección específica de cada interfaz, respectivamente.

Las siguientes líneas resaltadas de ese mismo comando show ipv6 route muestran información interesante sobre el siguiente salto en una ruta aprendida mediante RIP. El ejemplo resalta la ruta que va a la subred 3, y muestra la interfaz saliente S0/0/1, pero la dirección del siguiente salto es la dirección IP local de enlace de R2, que es FE80::213:19FF:FE7B:5026. Los protocolos de enrutamiento IPv6 publican normalmente las direcciones locales de enlace como direcciones de siguiente salto.

Finalmente, la última parte del ejemplo muestra la salida del comando show ipv6 interface brief, que enumera las direcciones IP de unidifusión de cada interfaz. Las líneas resaltadas muestran primero la dirección local de enlace (que empieza por FE8) y después la dirección de unidifusión global de la interfaz Fa0/0 de R1. Todas las interfaces que se utilizan en este ejemplo tienen tanto la dirección local de enlace, que se ha generado automáticamente, como la dirección de unidifusión global, según se muestra en la primera parte del Ejemplo 17.2.

La configuración de nombres de host y de servidores DNS en los routers IPv4 puede ser relativamente cómoda, pero para IPv6 puede muy bien llegar a ser una necesidad. Como consecuencia de la longitud de las direcciones IPv6, hasta un sencillo comando ping exige escribir bastante y hay que hacer referencia a la salida de otro comando, o a la documentación. Por tanto, tal como ocurría en IPv4, quizá sea conveniente configurar unos nombres de host estáticos en los routers, o hacer alusión a un servidor DNS, mediante los dos comandos siguientes. Obsérvese que los comandos y la sintaxis son los mismos que para IPv4, pero empleando direcciones IPv6 como parámetros.

- ip host *nombre dirección-ipv6* [*segunda-dirección*[*tercera dirección* [*cuarta-dirección*]]]
- ip name-server *dirección-servidor1* [*dirección-servidor2...dirección-servidor6*]

El primer comando configura un nombre de host que sólo es conocido para los routers locales, mientras que el segundo se refiere a un servidor DNS. Obsérvese que el router intenta actuar como cliente DNS de forma predeterminada, basándose en el comando de configuración global ip domain-lookup predeterminado. Sin embargo, si se ha configurado el comando no ip domain-lookup, hay que volver a cambiar el comando por ip domain-lookup para empezar a utilizar los servicios de DNS.

Aunque los comandos de configuración y show que hay en el Ejemplo 17.2 pueden resultar útiles para aprender las bases, se necesita mucho más antes de que una red pueda estar preparada para desplegar IPv6. (*Deploying IPv6 Networks*, escrito por Ciprian Popoviciu y otros, y publicado por Cisco Press, es un excelente recurso para quienes deseen leer algo más.) La sección siguiente examina brevemente uno de los problemas de despliegue más graves, que es la forma de soportar a los usuarios durante una migración mundial de IPv4 a IPv6, migración que puede durar décadas.

Opciones para la transición a IPv6

Aunque IPv6 resuelve un montón de problemas, pensar en una migración de IPv4 a IPv6 de la noche a la mañana es algo ridículo. El número de dispositivos que utilizan IPv4 es del orden de miles de millones, y en algunos casos, aunque se quisiera migrar a IPv6, los dispositivos o el software podrían muy bien no admitir IPv6, o por lo menos no tendrían un soporte bien probado para IPv6. La migración de IPv4 a IPv6 requerirá como mínimo años, si no son décadas.

Afortunadamente, se ha invertido mucho tiempo y esfuerzo en pensar sobre el proceso de migración, y en desarrollar estándares relativos a la forma de enfocar el problema de la migración o transición. Las secciones siguientes presentan las opciones principales y explican las bases. En particular, estas secciones examinan la idea de utilizar pilas duales, con túneles y conversiones entre ambas versiones de IP. Obsérvese que ninguna solución basta para resolver todos los problemas; con toda probabilidad, se necesitará una combinación de estas herramientas en casi todas las redes.

Pilas duales IPv4/IPv6

El término **pilas duales** significa que el elemento o router utiliza tanto IPv4 como IPv6 al mismo tiempo. Para los hosts, esto significa que se tiene tanto una dirección IPv4 como una dirección IPv6 asociada a cada tarjeta de red; que el host puede enviar paquetes IPv4 a otros hosts IPv4 y que el host puede enviar paquetes IPv6 a otros hosts IPv6. Para los routers, significa que además de las direcciones IP IPv4 habituales, y además de los protocolos de enrutamiento tratados en muchos de los otros capítulos de este libro, los routers también tendrían que tener direcciones IPv6 y protocolos de enrutamiento, como se ha mostrado en este capítulo. Para admitir tanto los hosts IPv4 como los IPv6, el router podría recibir y enviar tanto paquetes IPv4 como paquetes IPv6.

La metodología de las pilas duales puede ser un plan de ataque razonable para migra una empresa a IPv6 a efectos de las comunicaciones dentro de la empresa. Los routers se podrían migrar fácilmente al uso de pilas duales, y la mayoría de los sistemas operativos de sobremesa admiten IPv6 en la actualidad. En algunos casos, la actualización podría exigir nuevo software o hardware, pero este método permite una migración más lenta, lo cual no es necesariamente malo, porque el personal de soporte necesita tiempo para aprender la forma en que funciona IPv6.

Túneles

Otra herramienta para soportar la transición IPv4-IPv6 son los túneles. Existen muchas clases de túneles, pero en este caso la función de túnel típicamente admite un paquete IPv6 enviado por un host y lo encapsula dentro de un paquete IPv4. El paquete IPv4 se puede reenviar entonces a través de una red IPv4 ya existente, y otro dispositivo se encargará de descartar el encabezado IPv4, revelando así el paquete IPv6 original. El concepto es muy parecido al de un túnel VPN, como se explicaba en el Capítulo 15, “Redes privadas virtuales”.

La Figura 17.11 muestra un ejemplo típico de un túnel que se denomina genéricamente túnel de IPv6 a IPv4, lo cual significa IPv6 dentro de IPv4. La figura muestra un ejemplo de red empresarial en la cual los hosts de algunas de las LANs han migrado a IPv6, pero el grueso de la red sigue funcionando en IPv4. Esto podría suceder durante la fase inicial de pruebas de la empresa, o se podría hacer de forma común con un ISP basado en IPv4 que tuviera clientes deseosos de migrar a IPv6.

En la figura, el elemento PC1, que está basado en IPv6, envía un paquete IPv6. Entonces el router R1 encapsula o envía por el túnel el paquete IPv6 en un nuevo encabezado IPv4, tomando como destino la dirección IPv4 de una dirección del Router R4. Los Routers R2 y R3 reenvían tranquilamente el paquete, porque tiene un encabezado IPv4 normal, y R4 desencapsula el paquete original IPv6, reenviándolo al PC2 basado en IPv6. Esto se denomina un túnel, en parte porque los paquetes IPv6 que viajan por el túnel no se pueden ver mientras lo recorren; los routers situados en puntos intermedios de la red, que en este caso son R2 y R3, perciben los paquetes como paquetes IPv4.

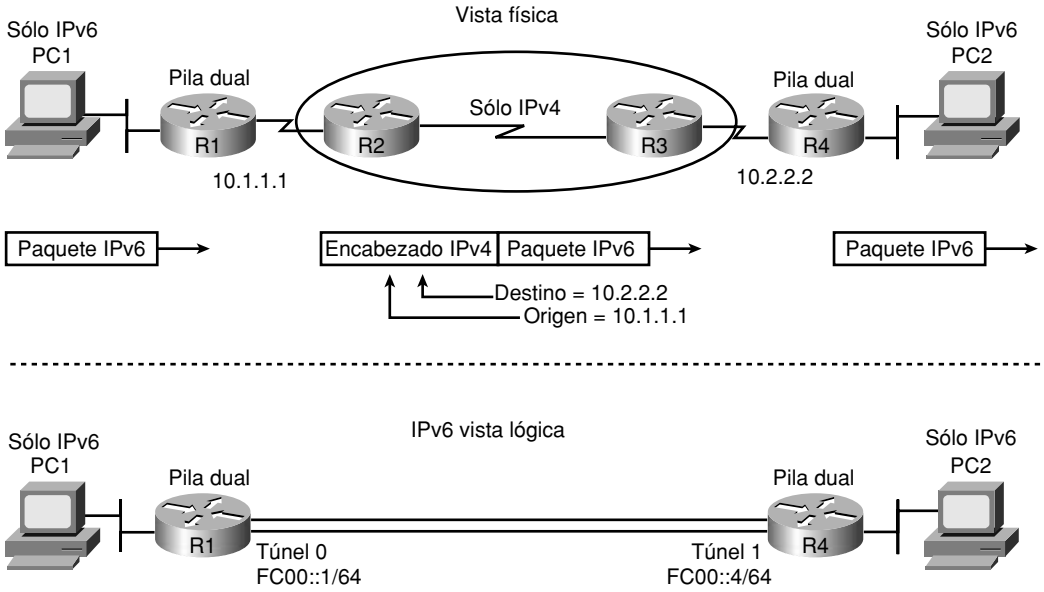


Figura 17.11. Ejemplo de túnel de IPv6 a IPv4: vista física y lógica.

Existen varios tipos de túneles de IPv6 a IPv4. Para construir un túnel como el que se muestra en los routers de la Figura 17.11, se podrían emplear los tres primeros tipos que se muestran a continuación; el cuarto tipo (túneles Teredo) lo emplean los hosts:

- **Túneles configurados manualmente (*Manually configured tunnels*, MCT).** Una configuración sencilla en la que se crean interfaces de túnel, una especie de interfaz de router virtual, con una configuración que hace referencia a las direcciones IPv4 empleadas en el encabezado IPv4 que encapsula el paquete IPv6.
- **Túneles dinámicos 6to4**. Este término se refiere a un tipo específico de túnel que se crea dinámicamente; esto se hace normalmente en las interfaces IPv4, en las que las direcciones IPv4 de los extremos del túnel se pueden hallar dinámicamente basándose en la dirección de destino IPv6.
- **Protocolo de direccionamiento de túneles automático intrasede (*Intra-site Automatic Tunnel Addressing Protocol*, ISATAP).** Otro método dinámico de creación de túneles, que normalmente se emplea dentro de las empresas. A diferencia de los túneles 6to4, los túneles ISATAP no funcionan si se utiliza NAT IPv4 entre extremos del túnel.
- **Túnel Teredo.** Este método permite a hosts dotados de pila dual crear túneles que llegan a otro host, de tal modo que el propio host crea el paquete IPv6 y lo encapsula en un encabezado IPv4.

La Figura 17.12 muestra la idea básica que subyace al túnel Teredo.

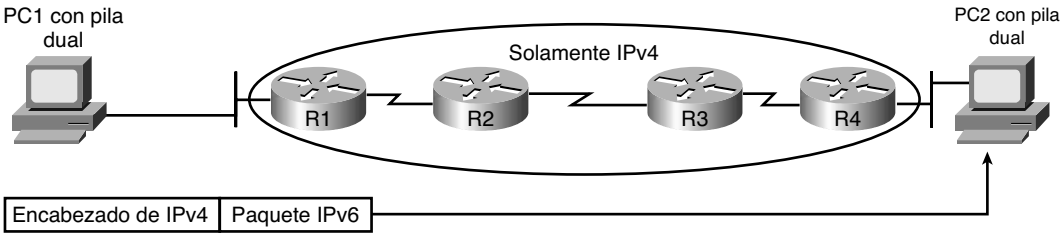


Figura 17.12. Ejemplo de encapsulación para un túnel Teredo de host a host.

Conversión entre IPv4 e IPv6 por medio de NAT-PT

Las dos clases de características de transición a IPv6 que se han mencionado hasta el momento en este capítulo, a saber, la pila dual y los túneles, se basan en que los hosts de los extremos admitan como mínimo IPv6, o bien tanto IPv4 como IPv6. Sin embargo, en ciertos casos, host que sólo admite IPv4 necesita comunicarse con un host que sólo dispone de IPv6. En este caso es preciso emplear una tercera clase de características de transición: una herramienta que convierte los encabezados de los paquetes IPv6 para que tengan el aspecto de un paquete IPv4, y viceversa.

En los routers de Cisco se puede utilizar la Conversión de direcciones de red y conversión de protocolo (*Network Address Translation–Protocol Translation*, NAT-PT), que está definida en la RFC 2766, para realizar la conversión. Para realizar este trabajo, un router configurado con NAT-PT debe conocer qué dirección IPv6 se traduce como qué dirección IPv4, y viceversa; es el mismo tipo de información que se almacena en una tabla tradicional de conversión NAT. Y al igual que la NAT tradicional, NAT-PT admite definiciones estáticas, NAT dinámica y PAT dinámica, que se puede utilizar para conservar direcciones IPv4.

Resumen de la transición

La Tabla 17.11 resume las opciones de transición a IPv6, para facilitar su estudio y como referencia.

Tabla 17.11. Resumen de las opciones de transición a IPv6.

Nombre	Tipo particular	Descripción
Pila dual	—	Admite ambos protocolos y envía IPv4 a hosts IPv4, e IPv6 a hosts IPv6.
Túnel	MCT	El túnel se configura manualmente; envía IPv6 a través de la red IPv4, típicamente entre routers.
Túnel	6to4	Los extremos del túnel se descubren dinámicamente; envía IPv6 a través de la red IPv4, típicamente entre routers.
Túnel	ISATAP	Los extremos del túnel se descubren dinámicamente, envía IPv6 a través de la red IPv4 entre routers; no admite NAT IPv4.
Túnel	Teredo	Normalmente lo utilizan los hosts; el host crea un paquete IPv6 y lo encapsula en IPv4.
NAT-PT	—	El router traduce entre IPv4 e IPv6; permite a los hosts IPv4 comunicarse con hosts IPv6.

Ejercicios para la preparación del examen

Repaso de los temas clave

Repase los temas más importantes del capítulo, etiquetados con un icono en el margen exterior de la página. La Tabla 17.12 especifica estos temas y el número de la página en la que se encuentra cada uno.

Tabla 17.12. Temas clave del Capítulo 17.

Tema clave	Descripción	Número de página
Figura 17.1	Conceptos de agregación de rutas en la Internet IPv6 global.	587
Lista	Reglas para abreviar las direcciones IPv6.	589
Lista	Reglas para escribir prefijos IPv6.	591
Figura 17.3	Ejemplo del proceso de asignación de prefijos.	593
Lista	Pasos principales para subdividir un prefijo en un prefijo de subred en una empresa.	595
Figura 17.5	Ejemplo y estructura de las subredes IPv6.	595
Figura 17.7	Estructura de las direcciones IPv6 e ID de interfaz con formato EUI-64.	600
Tabla 17.6	Lista de las cuatro opciones principales de configuración de direcciones IPv6.	604
Tabla 17.7	Comparaciones de los servicios IPv6 de DHCP con y sin estado.	606
Lista	Distintos tipos y propósitos de las direcciones IPv6.	606
Figura 17.10	Formato y estructura de las direcciones locales de enlace.	608
Lista	Resumen de los pasos que da un host para aprender su dirección, longitud de prefijo, DNS y router predeterminado.	609-610

(continúa)

Tabla 17.12. Temas clave del Capítulo 17 *(continuación).*

Tema clave	Descripción	Número de página
Tabla 17.9	Resumen de los prefijos y propósitos de los tipos más comunes de direcciones IPv6.	610
Lista	Lista de comprobación para la configuración de IPv6.	612
Tabla 17.11	Lista de opciones de transición a IPv6.	619

Complete de memoria las tablas y las listas

Imprima una copia del Apéndice J, "Ejercicios de memorización" (disponible en el DVD) o por lo menos de la sección de este capítulo, y complete de memoria las tablas y las listas. El Apéndice K, "Respuestas a los ejercicios de memorización", también disponible en el DVD, incluye las tablas y las listas completas para validar su trabajo.

Definiciones de los términos clave

Defina los siguientes términos clave de este capítulo y compruebe sus respuestas en el glosario:

Autoconfiguración sin estado, DHCP con estado, DHCP sin estado, dirección de unidifusión global, dirección local de enlace, dirección local exclusiva, NAT-PT, Pilas duales, prefijo de ISP, prefijo de registro, prefijo de sede, prefijo de subred, Protocolo de descubrimiento de vecindad (NDP), Registro regional de Internet (RIR).

Referencias de comandos

Aunque no necesariamente debe memorizar la información de las tablas de esta sección, ésta incluye una referencia de los comandos de configuración y EXEC utilizados en este capítulo. En la práctica, debería memorizar los comandos como un efecto colateral de leer el capítulo y hacer todas las actividades de esta sección de preparación del examen. Para verificar si ha memorizado los comandos como un efecto colateral de sus otros estudios, cubra el lado izquierdo de la tabla con un pedazo de papel, lea las descripciones en el lado derecho y compruebe si recuerda el comando.

Tabla 17.13. Comandos de configuración del Capítulo 17.

Comando	Descripción
ipv6 unicast-routing	Comando global que habilita el enrutamiento IPv6 en el router.
ipv6 router rip *etiqueta*	Comando global que habilita RIPng.
ipv6 rip *nombre* enable	Subcomando de interfaz que habilita RIPng en la interfaz.
ipv6 address {*dirección-ipv6/longitud-prefijo* | *nombre-prefijo sub-bits/longitud-prefijo*} eui-64	Subcomando de interfaz que configura manualmente o bien toda la dirección IP de la interfaz, o un prefijo /64 de modo que el router construya automáticamente el ID de interfaz con formato EUI-64.
ipv6 host *nombre dirección-ipv61* [*dirección-ipv62...dirección-ipv64*]	Comando global para crear una definición estática de nombre de host.
ip name-server *dirección-servidor1* [*dirección-servidor2...dirección-servidor6*]	Comando global para señalar uno o más servidores de nombres, con objeto de resolver el nombre en forma de direcciones IPv4 o IPv6.
[no] ip domain-lookup	Comando global que habilita el router como cliente DNS, o con la opción no, que deshabilita el router como cliente DNS.

Tabla 17.14. Comando EXEC del Capítulo 17.

Comando	Descripción
show ipv6 route	Muestra las rutas IPv6.
show ipv6 route *dirección-ip*	Muestra la ruta o rutas que emplearía este servidor para los paquetes enviados a la dirección indicada.
show ipv6 route [*prefijo/longitd-prefijo*]	Muestra la ruta correspondiente al prefijo /longitud indicado específicamente.
show ipv6 interface [*tipo número*]	Muestra la configuración IPv6 en una interfaz, incluyendo las direcciones de enlace local y otras direcciones IP de unidifusión.
show ipv6 interface brief	Muestra el estado de la interfaz y las direcciones IPv6 de cada una de las interfaces.

PARTE VI

Preparación final

Capítulo 18 Preparación final

cisco

CAPÍTULO 18

Preparación final

Los 17 primeros capítulos de este libro tratan las tecnologías, protocolos, comandos y características que es necesario comprender para aprobar el examen de ICND2. Aunque estos aportan la información detallada, casi todo el mundo necesita más preparación que limitarse a leer los 17 primeros capítulos. Este capítulo detalla un conjunto de herramientas y un plan de estudio que le servirán de ayuda para completar su preparación para los exámenes.

Si está preparando el examen de CCNA leyendo este libro y la guía **CCENT/CCNA ICND1**, ya sabrá que ambos libros tienen un capítulo de preparación final. Sin embargo, se puede hacer uso de este capítulo sin otra intención que leer el plan de estudios sugerido, ya que este capítulo se refiere a las herramientas aportadas tanto en este libro como en la guía **ICND1**. Sólo hay que buscar el texto que esté resaltado en gris, como esta frase, para encontrar las sugerencias aplicables a la preparación del examen CCNA (640-802), pero no a la preparación del examen ICND2 (640-816).

Este breve capítulo tiene dos secciones principales. La primera sección muestra las herramientas para la preparación del examen que pueden resultar útiles en este momento del proceso de estudio. La segunda sección muestra una sugerencia de plan de estudio ahora que ya se han completado los capítulos anteriores.

NOTA

Este capítulo hace referencia a muchos de los capítulos y apéndices del libro, así como a herramientas que están disponibles en el DVD. Algunos de los apéndices, a partir del Apéndice D, sólo están incluidos en el DVD que se ofrece junto con el libro. Para acceder a ellos, basta insertar el DVD y efectuar la selección adecuada en la interfaz que aparece al abrirlo.

Herramientas para la preparación final

Esta sección ofrece información relativa a las herramientas disponibles, y muestra la forma de acceder a ellas.

Cisco CCNA Prep Center

Cisco ofrece una amplia gama de herramientas de preparación de CCNA en un sitio web denominado CCNA Prep Center. El CCNA Prep Center ofrece demostraciones de la interfaz de usuario del examen, ejemplos de preguntas, vídeos informativos y otras herramientas.

Para utilizar el CCNA Prep Center, es necesario registrarse en http://www.cisco.com. Para ello, basta acceder a http://www.cisco.com, hacer clic en Register en la parte superior de la página y aportar algo de información. (No es necesario trabajar para Cisco o para alguno de sus asociados para obtener una cuenta.)

Una vez registrado, pase a http://www.cisco.com/go/prepcenter, y busque el enlace de CCNA Prep Center. Una vez allí, puede conectarse y explorar sus múltiples posibilidades.

Vídeos sobre *subnetting*, páginas de referencia y problemas de práctica

Es posible que la capacidad individual más importante para todos los exámenes de CCNA sea la de analizar el direccionamiento y el *subnetting* IP que se utilizan en las redes IPv4. El Capítulo 12 de la guía **CCENT/CCNA ICND1** trata la mayor parte de estos detalles, y el Capítulo 5 de este libro añade información mediante un examen de VLSM. (Si no tiene el libro de **ICND1**, el capítulo 12 de ICND1 se incluye en este libro en el Apéndice H, "ICND1 Chapter 12: IP Addressing and Subnetting", disponible en el DVD).

Este libro incluye varias herramientas que sirven para practicar y refinar nuestras capacidades en la creación de subredes:

- **Páginas de referencia de *subnetting*:** en el Apéndice E, disponible en el DVD y titulado "Subnetting Reference Pages", resume los procesos abreviadas para trabajar en binario y decimal que se explican en el Capítulo 12 de la guía **ICND1** y en el Capítulo 5 de este libro. Cada página de referencia muestra un único proceso relacionado con las subredes, junto con la función de referencia útil para ese proceso. Estos procesos resumidos pueden ser una herramienta cómoda cuando se están practicando el *subnetting*, en comparación con ir pasando páginas en los capítulos de subredes, en busca del proceso correcto.
- **Vídeos de subredes:** el DVD que se incluye en este libro contiene una serie de vídeos de subredes. Estos vídeos muestran la forma de utilizar los procesos abreviados para obtener las respuestas de cuestiones frecuentes en la creación de subredes. Se pueden seleccionar y reproducir los vídeos desde un sencillo menú que aparece cuando se inserta el DVD en un lector de DVD.
- **Prácticas de *subnetting*:** el Apéndice D "Subnetting Practice", que está disponible en el DVD, contiene toda una gama de problemas de prácticas de subredes, incluyendo 25 problemas para los cuales es necesario hallar el número de subred, la dirección de difusión de subred, y el rango de direcciones IP válidas. Este apéndice

muestra la forma de utilizar procesos tanto binarios como abreviados para obtener las respuestas.

Escenarios

Como se ha mencionado en la presentación del libro, algunas de las preguntas de examen requieren que uno tenga las mismas capacidades que normalmente se emplean para la resolución de problemas en redes reales. Las secciones y capítulos de resolución de problemas de ICND1 e ICND2 sirven de ayuda para prepararnos para esos tipos de cuestiones.

Otra forma de prepararse para las cuestiones de resolución de problemas que aparecen en los exámenes consiste en considerar mentalmente muchos escenarios de redes, prediciendo lo que debería ocurrir e investigando si la red se comporta como debería. El Apéndice F, "Additional scenarios", aparece tanto en este libro como en la guía **ICND1**, e incluye varios escenarios que a su vez muestran tareas que deberían realizarse antes de leer las soluciones que se sugieren más adelante en el apéndice. Al leer estos escenarios y hacer los ejercicios, se pueden practicar algunas de las capacidades que se requieren cuando se analizan redes y se resuelven sus problemas.

Plan de estudio

Sería posible limitarse a estudiar todas las herramientas disponibles, según se mencionaba anteriormente en este capítulo. Sin embargo, esta sección sugiere un determinado plan de estudio con una cierta sucesión de tareas que quizá resulte preferible a utilizar aleatoriamente las herramientas. Sin embargo, le recomendamos utilizar las herramientas de cualquier modo y en cualquier momento que le ayude a prepararse lo mejor posible para el examen.

Si sólo se va a preparar para el examen ICND2, puede ignorar las partes del plan de estudio que están marcadas en gris. Si va a estudiar para el examen CCNA empleando también el libro **ICND1**, incluya también las tareas marcadas en gris.

El plan sugerido agrupa las tareas en cuatro categorías:

- **Recuerde los hechos.** Actividades que sirven de ayuda para recordar todos los detalles de los 17 primeros capítulos del libro.
- **Prácticas con subredes.** Para tener éxito en los exámenes ICND1, ICND2 y CCNA es preciso dominar la creación de subredes. Esta categoría enumera los elementos que se pueden emplear para hacer prácticas de *subnetting*.
- **Aprenda a resolver problemas empleando escenarios.** Para responder a algunas cuestiones de examen que presentan un escenario, quizá necesite recordar hechos, hacer la aritmética de subredes de forma rápida y precisa, y utilizar un simulador práctico; y todo esto para responder a una sola pregunta. Esta sección del plan sugiere actividades que pueden servirle de ayuda para adquirir esta colección de capacidades diferentes.

Recuerde los hechos

Tal como sucede con la mayoría de los exámenes, es preciso recordar muchos hechos, conceptos y definiciones para hacer bien la prueba. Esta sección sugiere un par de tareas que le ayudarán a recordar todos los detalles:

Paso 1 **Revise y repita cuantas veces sea preciso las actividades de la sección "Ejercicios para la preparación del examen" que hay al final de todos los capítulos.** La mayoría de esas actividades le ayudará a refinar sus conocimientos de un cierto tema, y también le servirá para memorizar los hechos. Para la preparación del examen **CCNA**, haga esto para los Capítulos del 2 al 17 en el libro **ICND1**, y también en los capítulos del 1 al 17 de este libro.

Paso 2 **Revise todas las preguntas del cuestionario "Ponga a prueba sus conocimientos" que hay al principio de los capítulos.** Aunque las cuestiones puedan ser familiares, leerlas de nuevo puede servir de ayuda para recordar los temas tratados en las cuestiones. Además, las preguntas del cuestionario suelen tratar los temas más importantes del capítulo, y nunca está de más repasar estos temas.

Prácticas de *subnetting*

Sin la menor duda, la capacidad más importante que se necesita para tener éxito en los exámenes ICND1, ICND2 y CCNA consiste en ser capaz de responder a preguntas de subredes de forma precisa, con confianza y con rapidez. Los exámenes CCNA tienen todos unos ciertos factores de presión de tiempo; las cuestiones que causan más problemas son las *sim, simlet* y las relativas a las subredes. Por tanto, hay que practicar los procesos y la aritmética de subredes hasta que uno es capaz de hallar siempre la respuesta correcta en un tiempo razonable.

Antes de sugerirle la forma en que debe prepararse para las cuestiones relativas a las subredes, le rogamos que tenga en cuenta que hay muchos métodos alternativos para hallar las respuestas de estas preguntas. Por ejemplo, se puede emplear la aritmética binaria para los 32 bits de los números de direcciones y de subredes. Alternativamente, puede tener en cuenta que 3 de los cuatro octetos de la mayoría de los problemas de subredes se pueden predecir fácilmente sin aritmética, y utilizar la aritmética binaria en el octeto final, que es el que interesa. Otra opción sería emplear abreviaturas decimales. (Este tema se trata en el Capítulo 12 de **ICND1** y en el Apéndice H del libro.) Las abreviaturas no requieren aritmética binaria, pero sí requieren practicar un proceso hasta haberlo memorizado. Se puede, incluso, emplear variantes de estos procesos, tal como se enseñan en otros libros o en otras clases.

Sea cual sea el proceso preferido, es preciso practicarlo hasta que uno pueda utilizarlo de forma precisa, con confianza y con rapidez.

La siguiente lista de actividades sugeridas incluye actividades prácticas que se pueden emplear independientemente del proceso seleccionado. En algunos casos, la lista incluye cosas que sirven de ayuda para aprender los procesos abreviados que se incluyen en este libro:

Paso 1 **Lea o imprima el Apéndice E, "Subnetting Reference Pages".** Este breve apéndice, que sólo está disponible en el DVD, incluye una serie de resúmenes de una sola página relativos a los procesos de creación de subredes que se encuentran en el Capítulo 12 de **ICND1** (y en el Apéndice H de este libro, que es una copia del Capítulo 12 de **ICND1**). El Apéndice E contiene páginas de referencia que resumen los procesos de creación de subredes, tanto en su versión binaria como en la decimal.

Paso 2 **Visione los vídeos de creación de subredes que hay en el DVD.** Estos vídeos muestran ejemplos de la forma de utilizar algunos de los procesos abreviados más complejos para ayudarle a asegurarse de que sabe usar estos procesos. Candidatos al examen CCNA: los vídeos de subredes están en los DVDs que contienen los dos libros. Son idénticos, así que se pueden ver los vídeos de cualquiera de estos DVDs.

Paso 3 **Vea o imprima el Apéndice D, "Subnetting Practice".** Este apéndice, que sólo está disponible en el DVD, incluye una buena cantidad de problemas prácticos de subredes con objeto de que, por repetición, pueda mejorar significativamente su velocidad y asimilar los procesos abreviados. Cuente con trabajar en estos problemas hasta que siempre obtenga la respuesta correcta, con rapidez, y sin tener que sentarse a pensar acerca del proceso que se sigue para obtener la respuesta. Nuestro objetivo es hacer que el proceso para hallar las respuestas de estos problemas llegue a ser automático.

Candidatos al examen CCNDA: el Apéndice D de ICND2 contiene todos los problemas que hay en el Apéndice D de ICND1, y algunos más, así que se debe utilizar el Apéndice D de ICND2.

Paso 4 **Prácticas con subredes empleando el Subnetting Game de Cisco.** Cisco tiene un juego de creación de subredes, que está disponible en el CCNA Prep Center. El juego va presentando distintos escenarios de subredes y hace divertida la práctica con subredes. Acceda al CCNA Prep Center (http://www.cisco.com/go/prepcenter), conéctese con su cuenta de usuario de Cisco.com, seleccione la ficha Additional Information y busque el enlace para descargar el juego. (Si no tiene una cuenta puede crearla desde esta misma página web.)

Paso 5 **Desarrolle sus propios problemas de prácticas empleando una calculadora de subredes.** Es posible descargar muchas calculadoras de subredes en Internet, incluyendo una que está disponible en Cisco como parte del CCNA Prep Center. Se pueden crear problemas de subredes propios como los del Apéndice D, para después hacer los problemas y comprobar las respuestas empleando la calculadora de subredes.

Aprenda a resolver problemas empleando escenarios

Del mismo modo que un problema real de una red real puede darse por muchas causas (un protocolo de enrutamiento, un cable defectuoso, el árbol de extensión, una ACL inco-

rrecta, e incluso errores en la documentación de la red) el examen nos obliga a aplicar una amplia gama de conocimientos para responder a preguntas individuales. La única actividad de esta sección es la siguiente:

- **Revisar los escenarios incluidos en el Apéndice F del libro.** Estos escenarios nos hacen pensar sobre temas tratados en muchos capítulos del libro. Además, requieren un pensamiento más abstracto para resolver el problema. Los candidatos al examen CCNA deben revisar los escenarios del Apéndice F de ambos libros.

Resumen

Las herramientas y sugerencias que se muestran en este capítulo se han diseñado con un objetivo: ayudarle a desarrollar las capacidades necesarias para aprobar los exámenes ICND2 y CCNA. Este libro, y el libro **ICND1** con el que forma pareja, no sólo se han desarrollado para aportar los hechos, sino también para que sirvan de ayudar a la hora de aplicar esos conocimientos. Sea cual fuere el nivel de experiencia que se tenga cuando se intente pasar el examen, esperamos que la amplia gama de herramientas de preparación, e incluso la estructura de los libros y el énfasis con que se aborda la resolución de problemas, permitan al lector superarlo con facilidad. Le deseamos mucha suerte en los exámenes.

PARTE VII

Apéndices

Apéndice A Respuestas de los cuestionarios "Ponga a prueba sus conocimientos"

Apéndice B Tabla de conversión de decimal a binario

Apéndice C Actualizaciones del examen ICND2: Versión 1.0

Glosario

cisco

APÉNDICE A

Respuestas de los cuestionarios "Ponga a prueba sus conocimientos"

Capítulo 1

1. B
2. D. Aunque los conceptos de subred y de VLAN no son equivalentes, los dispositivos de una VLAN están normalmente en la misma subred, y viceversa.
3. B
4. C
5. B y C
6. A y C. El ajuste auto significa que el switch puede negociar el *trunking*, pero sólo puede responder a mensajes de negociación y no puede iniciar el proceso de negociación. Por tanto, el otro switch debe estar configurado para actuar de forma troncal o para iniciar el proceso de negociación (basándose en que está configurado con la opción dynamic desirable.)
7. A. La configuración predeterminada de VTP, que es el modo servidor de VTP, significa que el switch puede configurar las VLANs, así que se configura la VLAN. Sin embargo, al estar en el modo de servidor, los comandos de configuración sólo aparecen en la salida del comando show vlan brief, y no se enumeran formando parte del archivo *running-config*.
8. B y C
9. C. VTP no requiere una contraseña, aunque si se utiliza una contraseña, entonces tienen que coincidir. VTP envía actualizaciones VTP inmediatamente después de que se produzcan cambios en una base de datos VLAN. Sin embargo, VTP sólo

envía mensajes VTP a través de troncales y de forma predeterminada los 2960 utilizan un modo administrativo troncal de auto, que no inicia el proceso de negociación de *trunking*. Por tanto, ninguno de los switches forma automáticamente una conexión troncal y no se envían mensajes VTP.

10. C y D. El nombre del dominio y la contraseña tienen que ser iguales, y los switches tienen que conectarse empleando una conexión troncal para que VTP pueda funcionar. Es normal hacer que algunos switches actúen como servidores y otros como clientes. Una configuración de *pruning* incorrecta no evita la sincronización de las bases de datos VLAN.

Capítulo 2

1. A y B. Los estados de escucha y aprendizaje (*Listening* y *Learning*) son estados transitorios de los puertos, que sólo se utilizan cuando se pasa del estado de bloqueo al de envío (*Blocking* y *Forwarding*, respectivamente). El estado de descarte (*Discarding*) no es un estado de puerto 802.1d STP.

2. C y D. Los estados de escucha y aprendizaje son estados transitorios de los puertos, que sólo se utilizan cuando se pasa del estado de bloqueo al de envío. El estado de descarte no es un estado de puerto 802.1d STP. *Forwarding* y *Blocking* son estados estables.

3. C. El ID numérico de puente más pequeño gana las elecciones.

4. B. Los switches que no son raíz envían los Hellos que reciben del raíz; el router raíz envía estos Hellos basándose en la configuración de su temporizador Hello.

5. E

6. B y D. El estándar IEEE 802.1w, que se denomina Rapid STP, ofrece una convergencia de STP mucho más rápida.

7. B y D. RSTP utiliza los estados de puerto *Forwarding*, *Learning* y *Discarding*, y los estados de *Forwarding* y *Learning* tienen la misma funcionalidad básica que los estados de puerto STP de igual nombre.

8. B y C

9. B. Los switches de Cisco utilizan el formato de ID de sistema extendido para los ID de puente de forma predeterminada; este formato es tal que el campo de prioridad se fragmenta en un valor base de la prioridad (32.768 en este caso) más el ID de VLAN. La prioridad de este switch le permite tener la capacidad de ser el switch raíz, pero el resultado del comando no aporta información suficiente para saber si este switch es o no el raíz en la actualidad.

10. B. Las dos interfaces tienen un coste de puerto predeterminado igual a 19 (Fa0/13) y 4 (Gi0/1), lo cual da lugar a que el coste de SW3 para alcanzar el raíz sea de 10 + 19 = 29 pasando por Fa0/13, y de 20 + 4 = 24 a través de Gi0/1. Por tanto, SW3 selecciona a Gi0/1 como puerto raíz. SW3 podría notificar entonces un coste de 24 (el coste necesario para llegar al router raíz) para un Hello que saliera por Fa0/13,

pero sería inferior al de un Hello que ya se está recibiendo en Fa0/13 (con coste 10), así que SW3 no seleccionaría a Fa0/13 como puerto designado.

Capítulo 4

1. D. El host podría tener necesidad de utilizar el Protocolo de configuración dinámica del host (DHCP) para conseguir una dirección IP, y probablemente utilizase el Sistema de denominación de dominio (DNS) para resolver www.ciscopress.com y conseguir su dirección IP. También utilizaría el Protocolo de resolución de direcciones (ARP) para obtener la dirección MAC del gateway predeterminado, porque la caché ARP habría resultado borrada como parte del proceso de arranque.
2. B. El comando ping 2.1.1.2 no utiliza un nombre de host, así que no se requiere un servidor DNS. El cliente DHCP no necesita conocer la dirección IP del servidor DHCP para utilizar DHCP. No existe tal cosa como un servidor ARP. Sin embargo, para enviar el paquete a otra subred, la computadora necesita conocer la dirección IP de su gateway predeterminada.
3. A y F
4. C. Una vez configurado el comando no ip subnet-zero, el router no permitirá que ninguna interfaz se configure con una dirección IP perteneciente a la subred cero. De las respuestas mostradas, la subred 10.0.0.0 255.254.0.0 es una subred cero, con un rango de direcciones que va desde 10.0.01 hasta 10.1.255.254. El comando ip address 10.1.2.2 255.254.0.0 sería rechazado.
5. C. El código "S" significa que la ruta es estática, lo cual se habrá definido con el comando de configuración global ip route.
6. A. La sintaxis correcta muestra un número de subred, después una máscara de subred en formato decimal con puntos, y luego o bien una interfaz saliente o una dirección IP de siguiente salto.
7. A
8. B. Una vez activado el enrutamiento sin clase, el router utiliza la ruta predeterminada si no vale ninguna otra. La línea que empieza con las palabras "Gateway of last resort..." (gateway de último recurso) muestra la dirección IP del router de siguiente salto, 168.13.1.101, que se utilizará como ruta predeterminada.

Capítulo 5

1. B, C y D
2. A. Obsérvese que en ciertas ocasiones VLSM significa enmascaramiento de subred de longitud variable, que se refiere al proceso consistente en utilizar distintas más-

caras en una misma red con clase, mientras que la máscara de subred de longitud variable se refiere a las máscaras de subred en sí.

3. C y D. La subred 10.5.0.0 255.255.240.0 implica el rango 10.5.0.0–10.5.15.255, que no se solapa. 10.4.0.0 255.254.0.0 implica el rango 10.4.0.0–10.5.255.255, que sí se solapa. 10.5.32.0 255.255.224.0 implica el rango 10.5.32.0–10.5.63.255, que sí se solapa. 10.5.0.0 255.255.128.0 implica el rango 10.5.0.0– 10.5.127.255, que sí se solapa.
4. C. Todas las respuestas enumeradas incluyen el rango de las tres subredes, salvo 10.3.64.0 255.255.224.0, que implica un rango de direcciones de 10.3.64.0–10.3.95.255. De las tres respuestas, 10.3.64.0 255.255.192.0 es el rango más pequeño (10.3.64.0–10.3.127.255). Además, también es la ruta de resumen individual más corta que incluye a las tres redes mostradas en la pregunta.
5. C y D. 10.0.0.0 255.0.0.0 implica un rango formado por todas las direcciones que empiezan por 10 y 10.1.0.0 255.255.0.0 implica un rango formado por todas las direcciones que empiezan por 10.1, así que estas dos respuestas incluyen todos los rangos de direcciones enumerados en la cuestión. 10.1.32.0 255.255.224.0 implica un rango de 10.1.32.0–10.1.63.255, que incluye todas las direcciones enumeradas en la cuestión. 10.1.55.0 255.255.255.0 implica un rango que sólo abarca 10.1.55.0–10.1.55.255, lo cual no incluye todas las direcciones. 10.1.48.0 255.255.248.0 implica un rango de 10.1.48.0–10.1.55.255, que omite dos de las subredes indicadas en la cuestión.
6. B, C y D
7. A, B y C
8. A. Se permiten las redes discontinuas siempre y cuando se inhabilite el autoresumen. OSPF ni siquiera admite el autoresumen, así que el uso de OSPF resolvería el problema. RIP-1 no puede inhabilitar el autoresumen. EIGRP puede inhabilitar el autoresumen, pero está activado de forma predeterminada.

Capítulo 6

1. A y C. Las ACLs estándar comprueban la dirección IP de origen. El rango de direcciones10.1.1.1– 10.1.1.4 se puede especificar mediante una ACL, pero requiere múltiples comandos access-list. Es posible especificar todos los hosts de la subred de Barney empleando el comando access-list 1 permit 10.1.1.0 0.0.0.255.
2. D. 0.0.0.255 especifica todos los paquetes que tienen iguales los tres primeros octetos. Esto resulta útil cuando se desea especificar una subred en la cual la parte de subred abarca los tres primeros octetos, como en este caso.
3. E. 0.0.15.255 especifica todos los paquetes que tienen iguales los veinte primeros bits. Esto es útil cuando se desea especificar una subred en la que la parte de subred abarca los 20 primeros bits, como en este caso.
4. E y F. Las ACLs extendidas pueden examinar los encabezados de capa 3 (IP) y de capa 4 (TCP, UDP) y unos pocos más, pero no llegan a la información de la capa de aplicación. Las ACLs extendidas y con nombre pueden buscar los mismos campos que las ACLs extendidas y numeradas.

5. A y E. El rango correcto de números de ACL para las listas de acceso IP extendidas es de 100 a 199 y de 2000 a 2699. Las respuestas que muestra el parámetro eq www después de 10.1.1.1 especifican el número de puerto de origen y los paquetes van hacia el servidor web, no vienen de él.

6. E. Como el paquete va hacia cualquier cliente web, es necesario comprobar el número de puerto del servidor como puerto de origen. El rango de direcciones IP de cliente no se especifica en la cuestión, pero se indican las de los servidores, así que la dirección de origen que empieza por 172.16.5 es la respuesta correcta.

7. E. Las ACLs IP extendidas y con nombre pueden especificar exactamente el mismo conjunto de campos que las ACLs IP extendidas y con número.

8. A y C. Con anterioridad al IOS 12.3, las ACLs con número deben ser descartadas y reconfiguradas para descartar una línea de la ACL. A partir del IOS 12.3, también se puede emplear el modo de configuración de ACL y unos números de secuencia para borrar una línea de ACL de cada vez.

9. C. El currículo autorizado de Cisco hace la indicación que hay en la respuesta C para las ACLs IP extendidas, sugiriendo que las ACLs estándar se pongan tan próximas al destino como sea posible.

10. C. Las ACLs dinámicas requieren que el usuario haga telnet al router y se autentique empleando un nombre de usuario y una contraseña, lo cual hará que el router admite los paquetes enviados por ese host.

Capítulo 8

1. A y B

2. D y F

3. C y D

4. B, C, D y E

5. B. Los protocolos por vector de distancia se basan en actualizaciones completas de encrutamiento enviadas periódicamente desde los vecinos para confirmar que el vecino sigue funcionando.

6. D. El horizonte dividido da lugar a que el router no publique las rutas a través de una interfaz si la ruta va a dar lugar a que se envíen paquetes a través de esa misma interfaz.

7. D. El envenenamiento de rutas significa publicar la ruta fallida como poseedora de una ruta "infinita", en lugar de limitarse a dejar de publicar esa ruta. El envenenamiento inverso es un envenenamiento de rutas debido a publicar una ruta que anteriormente no se hubiera publicado como consecuencia del horizonte dividido.

8. A. El router no debería enviar inmediatamente una actualización completa. En lugar de hacer esto, los protocolos por vector de distancia envían inmediatamente una actualización parcial de enrutamiento, que contiene únicamente la ruta envenenada.

9. B. Los protocolos por estado del enlace vuelven a llenar todas las LSAs con un temporizador periódico pero más largo. Cuando se emplea RIP, el temporizador de actualización es de 30 segundos, y con OSPF el temporizador es de 30 minutos.

10. B. Los protocolos por estado del enlace recopilan información relativa a la red en forma de LSAs, que se hallan en memoria en la base de datos de estado del enlace. El router ejecuta entonces el algoritmo SPF para calcular la ruta que tiene la mejor métrica en ese router para llegar a cada subred.

Capítulo 9

1. A. OSPF calcula las métricas basándose en el coste asociado a cada interfaz. De forma predeterminada, OSPF calcula el coste de la interfaz basándose en la configuración de ancho de banda.

2. A y D. OSPF utiliza el algoritmo SPF, que fue concebido por un matemático llamado Dijkstra.

3. A y D. Los routers tienen que emplear el mismo tipo de autenticación y, de ser así, la misma clave de autenticación. Además, el número de subred y el rango de direcciones, calculados a partir de las direcciones IP y las máscaras de las interfaces, tienen que estar en la misma subred.

4. B. Los routers OSPF vecinos que completan el intercambio de bases de datos se consideran completamente adyacentes y se hallan en un estado de vecindad completa.

5. D y E. El DR se elige basándose en la prioridad OSPF más elevada. Si hay un empate, se basa en el RID OSPF más alto. Sin embargo, una vez seleccionado el DR, el rol de DR no puede ser adoptado por un router mejor mientras el DR y el BDR no hayan perdido conectividad con la subred. El DR intenta ser completamente adyacente con los demás routers de la subred como parte del proceso optimizado de intercambio de bases de datos.

6. B. El comando `network 10.0.0.0 0.255.255.255 area 0` funciona, porque especifica todas las interfaces cuyo primer octeto es 10. El comando `network 10.0.0.1 0.255.255.0 area 0` utiliza una lógica de coincidencia que busca todas las interfaces cuyo primer octeto sea 10 y cuyo último octeto sea 1, lo cual denota las direcciones IP de las tres interfaces. Sin embargo, la máscara *wildcard* que se usa en los tres comandos `network` de OSPF sólo puede tener una serie de unos binarios consecutivos, con todos los demás dígitos iguales a 0 binario, y esta máscara *wildcard* viola esa regla.

7. A. El comando `network 0.0.0.0 255.255.255.255 area 0` especifica todas las direcciones IP como resultado de utilizar una máscara *wildcard* igual a 255.255.255.255, así que este comando activa OSPF en el área 0 de todas las interfaces. La respuesta que tiene la máscara *wildcard* 0.255.255.0 no es válida, porque representa más de una sucesión de ceros binarios separados por unos binarios. La respuesta que contiene las "x" es sintácticamente incorrecta. La respuesta que contiene la máscara *wildcard*

255.0.0.0 significa "Admitir todas las direcciones cuyos tres últimos octetos sean 0.0.0", así que no queda seleccionada ninguna de las tres interfaces.

8. A, B y E

9. B y D. Para que el estado de vecindad de R2 respecto a R3 sea completo, R2 y R3 tienen que haber pasado el proceso de autenticación tal como lo requiere la configuración de R2. La clave de autenticación tiene que haber sido configurada con el subcomando de interfaz `ip ospf authentication messagedigest-key`. Sin embargo, el tipo de autenticación no necesita ser configurado mediante el subcomando de interfaz `ip ospf authentication message-digest-key`. R1 se halla en el estado `Init` como consecuencia de uno de entre varios problemas que pueden suceder e impiden que se comuniquen los vecinos, así que no es posible determinar si el problema de R1 es un problema de autenticación.

10. D. El subcomando de router OSPF `maximum-paths` *número* especifica el número de rutas de igual coste que se añaden a la tabla de enrutamiento. De forma predeterminada, este comando tiene el valor 4.

Capítulo 10

1. A y B

2. D

3. B. La distancia factible (FD) es, para todas las rutas conocidas que llegan a una subred, la métrica de la mejor de esas rutas. La mejor ruta se denomina ruta sucesora y se añade a la tabla de enrutamiento IP.

4. C. La distancia informada (RD) de una ruta es la métrica utilizada por el vecino que ha publicado esa ruta. El router la utiliza para determinar qué rutas satisfacen la condición de viabilidad para saber si una ruta puede o no ser una ruta sucesora factible.

5. A y C. El comando EIGRP `network` admite como parámetro una red con clase, habilitando EIGRP en todas las interfaces de esta red con clase, o una dirección y una máscara *wildcard*. En el último caso, las direcciones IP de las interfaces que coincidan con la dirección configurada, al aplicar la lógica similar a la de ACL con la máscara *wildcard*, se verán afectadas por el comando.

6. C y D. El comando EIGRP `network 10.0.0.2 0.0.0.0` define exactamente la interfaz cuya dirección es 10.0.0.2 como consecuencia de la máscara *wildcard*, y habilita EIGRP en esa interfaz. El valor de ASN para EIGRP tiene que coincidir en ambos routers. El comando `network 10` es incorrecto sintácticamente; debe configurarse toda la red con clase en su totalidad.

7. C. El primer número que va entre paréntesis es la métrica calculada para una ruta, y el segundo número es la distancia notificada (RD) de la ruta. La ruta que pasa por 10.1.6.3 es la ruta sucesora, así que no es una ruta sucesora factible. Para las otras dos rutas, sólo la RD de la tercera ruta es menor o igual que la distancia factible (la métrica de la ruta sucesora).

8. B y D. Es preciso configurar la clave MD5. No se configura mediante un subcomando de interfaz, sino como parte de una cadena de claves. La vida útil de una clave se puede configurar, pero no es necesario.

9. F

Capítulo 12

1. C. De las respuestas posibles, sólo PAP y CHAP son protocolos de autenticación PPP. PAP envía la contraseña en formato de sólo texto entre los dos dispositivos.

2. C. El Protocolo para el control del enlace (LCP) PPP controla ciertas funcionalidades que se aplican al enlace independientemente del protocolo de capa 3, incluyendo la detección de enlaces cerrados, la monitorización de la calidad del enlace y la autenticación.

3. A y D. Ambos routers necesitan un comando `encapsulation ppp` y también los dos necesitarán direcciones IP antes de que pueda funcionar el `ping`. R1 no necesita un comando `clock rate`, porque R2 está conectado al cable DCE.

4. D. El comando `username` de un router debería referirse al nombre de host del otro router, respetando las mayúsculas y minúsculas.

5. B y D. La salida muestra una encapsulación PPP, lo cual significa que está configurado para utilizar PPP. El estado de línea y del protocolo es "*up*" en ambos casos, LCP está abierto y tanto CDPCP como IPCP están abiertos, lo cual significa que se pueden enviar paquetes IP y CDP a través del enlace.

6. C y D. Los problemas de la capa física dan lugar normalmente a que el estado de línea (el primer código de estado) tenga el valor "*down*". La dirección IP de un router remoto ubicado en una subred distinta no evitaría que una interfaz configurada con PPP alcanzase un estado de protocolo (que es la segunda línea de estado) con un valor de "*up*". Si el otro extremo del enlace se ha configurado equivocadamente para utilizar HDLC, o si se ha configurado para PPP pero ha fallado la autenticación CHAP, entonces la interfaz podría estar en un estado "*up* y *down*", tal como se muestra.

7. B. Con PPP, dos routers pueden utilizar direcciones IP situadas en distintas subredes en los dos extremos del enlace, y funcionaría un `ping` enviado a la dirección IP serie del otro router. Sin embargo, esta desigualdad de subredes da lugar a que fallen los protocolos de enrutamiento cuando se forman relaciones de vecindad para intercambiar rutas, así que ninguno de los routers va a aprender rutas EIGRP procedentes del otro router.

Capítulo 13

1. C. La LMI administra el enlace existente entre el DTE y el switch, y esto incluye detectar el momento en que un circuito virtual (VC) se activa o se desactiva.

2. A y D. Típicamente, el DTE se ubica en el sitio cliente y el DCE se ubica en el sitio del proveedor de servicios. Los switches Frame Relay envían mensajes LMI a los DTEs (que típicamente son routers) para notificar el estado de un VC. Las tramas de Frame Relay carecen de DLCI de origen y de destino; tienen únicamente un campo DLCI.

3. A

4. C. El DLCI denota un VC, no un router. El valor de DLCI que hay en la trama mientras ésta pasa por el enlace local representa al VC en ese enlace. Como la pregunta se refiere a una trama que cruza el enlace de acceso conectado a R1, 222 es el DLCI local en R1 que identifica a ese VC.

5. B y C. Los DLCI globales representan al DLCI que utilizan los otros routers cuando envían tramas a través de sus enlaces de acceso local. Por tanto, cuando R1 envía una trama a R2, y la trama pasa por el enlace de acceso de R2, la red ha modificado el DLCI para que sea el DLCI global de R1, que es 101. De forma similar, cuando R3 envía una trama a R1, y la trama cruza el enlace de acceso de R3, la trama contiene el DLCI global de R1, que es 101.

6. A. Se puede utilizar una sola subred en cualquier topología Frame Relay, pero con una malla completa, se puede utilizar una sola subred sin problemas relacionados con los protocolos de enrutamiento.

7. D. BarneyCo posee un total de diez VCs. Si se configuran todos ellos en subinterfaces punto a punto, se necesitan diez subredes, porque se necesita una subred por VC.

8. A. La trama que ha sufrido los efectos de la congestión iba desde R1 hasta R2, así que la trama que tiene activado el bit de *Backward* (dirección opuesta) *Explicit Congestion Notification* (BECN) iría en la dirección opuesta, de R2 hacia R2.

Capítulo 14

1. C. Las palabras reservadas correctas son `ansi` y `q933`. Sin embargo, los routers detectan el tipo de LMI de forma predeterminada, así que también funciona si no se configura la LMI.

2. C, D y E. El tipo de LMI se autodetecta de forma predeterminada. El ARP Inverso también está activado de forma predeterminada, lo cual significa que no es necesario habilitarlo mediante el comando `frame-relay inverse-arp`, y tampoco es preciso añadir sentencias de asignación estática.

3. A y E. La dirección IP pasa a la subinterfaz, así que es necesario eliminarla primero de la interfaz serie (mediante el comando `no ip address`). La encapsulación permanece en la interfaz física. Es preciso utilizar el comando `frame-relay interface-dlci` en la subinterfaz, para que el router sepa qué DLCI corresponde a qué subinterfaz, aun cuando exista un solo DLCI.

4. F. En un comando `frame-relay interface-dlci` sólo se puede configurar un DLCI, y se precisa uno por cada VC que haya en la interfaz multipunto.

5. F
6. C y E. *Up* y *down* no son códigos de estado PVC. *Inactive* significa que el switch piensa que un PVC definido no funciona, y *deleted* (borrado) significa que el DLCI no está definido en el switch.
7. D. Para que una subinterfaz Frame Relay se encuentre en un estado *up*/*up*, la interfaz física subyacente también tiene que estar en estado *up*/*up* y al menos uno de los PVCs asociados a la subinterfaz tiene que estar en uno de los dos estados operativos de los PVCs (*active* o *static*).
8. B y C. Para que una interfaz física de Frame Relay tenga un estado de línea "*up*", tienen que estar en funcionamiento las mismas características de capa física que las que se emplean en las líneas alquiladas. Para tener también un estado de protocolo "*down*", o bien en el router falta el comando encapsulation frame-relay, o el router y el switch no están de acuerdo en el tipo de LMI.

Capítulo 15

1. A. Las VPNs extranet conectan sitios ubicados en empresas distintas pero que cooperan. Las VPNs de acceso ofrecen acceso a usuarios individuales, normalmente desde su domicilio o cuando están de viaje. El término "VPN empresarial" no suele utilizarse para describir un tipo de VPN.
2. C. El software antivirus es una función de seguridad muy importante, pero no es una función que ofrezca la VPN en sí.
3. A y C. Los encabezados ESP admiten las cuatro funciones que se enumeran en las respuestas, mientras que el encabezado de autenticación (AH) sólo admite la autenticación del mensaje y verifica su integridad.
4. A. De estas respuestas, sólo DES, 3DES y AES son herramientas de encriptación para encriptar todo el paquete. AES ofrece una encriptación mejor y requiere menos tiempo de computación que las otras opciones.
5. A, D y E. Todos los dispositivos y el software que se muestran en las respuestas se pueden emplear para terminar un túnel VPN. Sin embargo, los ASAs han sido sustituidos por cortafuegos PIX y concentradores VPN en la línea de productos de Cisco.
6. A y C. El cliente siempre utiliza SSL para conectarse al servidor Web VPN, así que todas las comunicaciones con Internet están encriptadas. Una de las ventajas más importantes de Web VPN es que los clientes no necesitan tener software cliente, sino que se limitan a utilizar las capacidades de SSL que tienen incorporadas los navegadores web típicos.

Capítulo 16

1. F
2. D. El objetivo inicial de CIDR era permitir crear un resumen de múltiples redes de las Clases A, B y C para reducir el tamaño de las tablas de enrutamiento de Internet. De las respuestas, sólo la 200.1.0.0 255.255.0.0 resume múltiples redes.
3. B y E. La RFC 1918 identifica los números de red privados. Se incluye la red de Clase A 10.0.0.0, las redes de Clase B de la 172.16.0.0 a la 172.31.0.0 y las redes de Clase C de la 192.168.0.0 a la 192.168.255.0.
4. C. Cuando se emplea NAT estática, las entradas se configuran estáticamente. Como la cuestión menciona la conversión para direcciones internas, la palabra reservada inside es necesaria en el comando.
5. A. Cuando se emplea NAT dinámica, las entradas se crean como resultado del primer flujo de paquetes procedente de la red interna.
6. A. El parámetro list 1 hace referencia a una ACL IP, que localiza paquetes, identificando las direcciones locales internas.
7. E. Cuando se convierten direcciones internas, la dirección externa no se convierte, así que no es necesario identificar la dirección local externa en la configuración.
8. A y C. En la configuración falta la palabra reservada overload en el comando ip nat inside source y en el subcomando de interfaz ip nat outside de la interfaz serie.
9. B. La última línea menciona que el almacén tiene siete direcciones, y las siete están asignadas, con un contador de fallos próximo a 1000: esto significa que ha habido cerca de 1000 flujos rechazados como consecuencia de un espacio insuficiente en el almacén de NAT.

Capítulo 17

1. A. Un método para la asignación de direcciones de unidifusión globales en IPv6 consiste en que ICANN asigna grandes bloques de direcciones a los RIRs, y los RIRs asignan bloques de direcciones más pequeños a los ISPs, y los ISPs asignan bloques aún más pequeños a sus clientes.
2. D. Dentro de un cuarteto se pueden omitir los posibles ceros iniciales y se puede reemplazar una sucesión de uno o más cuartetos que sólo estén formados por ceros por dos signos de dos puntos (::). La respuesta correcta reemplaza la sucesión más larga, de tres cuartetos llenos de ceros, por ::.
3. D. Las direcciones globales de unidifusión comienzan por 2000::/3, que significa que los tres primeros bits coinciden con el valor hexadecimal 2000. De forma similar, las direcciones locales exclusivas coinciden con FD00::/8 y las direcciones locales de enlace con FE80::/10 (los valores que comienzan por FE8, FE9, FEA y FED en hexadecimal). Las direcciones IPv6 de multidifusión comienzan por FF00::/8, lo cual significa que los dos primeros dígitos hexadecimales son F.

4. A y C. IPv6 admite DHCP con estado, que funciona de forma similar al protocolo DHCP de IPv4 para asignar dinámicamente toda la dirección IP. La autoconfiguración sin estado también permite efectuar la asignación buscando el prefijo en algún router cercano y calcular el ID de interfaz empleando el formato EUI-64.

5. A y D. La autoconfiguración sin estado sólo ayuda al host a aprender y formar su propia dirección IP, pero no le ayuda a localizar un gateway predeterminado. RS sin estado no es un término válido para una característica. El *Neighbor Discovery Protocol* (NDP) se utiliza con varios propósitos, incluyendo la misma finalidad que ARP en IPv4 y para determinar parámetros de configuración como la dirección IP de gateway predeterminado.

6. A y D. OSPFv3, RIPng, EIGRP para IPv6 y MP-BGP4 soportan todos IPv6.

7. C y E. La configuración asigna explícitamente la dirección IP 3456::1. La interfaz también forma el ID de interfaz EUI-64 (6444:44FF:FE44:4444), añadiéndolo a FE80::/64, para formar la dirección IP local de enlace.

8. E. La configuración de RIPng no hace uso de un comando `network`; en lugar de hacer esto, se configura el comando `ipv6 rip` en la interfaz, y se emplea la misma etiqueta que en el comando `ipv6 router rip` y la palabra reservada `enable`.

9. D. El protocolo *Network Address Translation–Protocol Translation* (NAT-PT) traduce entre IPv4 y IPv6. Los dos métodos de creación de túneles permiten a hosts IPv6 comunicarse con otros hosts IPv6, enviando los paquetes a través de una red IPv4. La pila dual permite a un host o a un router admitir concurrentemente ambos protocolos.

cisco

APÉNDICE B

Tabla de conversión de decimal a binario

Este apéndice ofrece una cómoda referencia para convertir los números del 0 al 255 entre los formatos decimal y binario. Consulte esta tabla siempre que quiera practicar con cualquiera de los problemas de subredes que hallará en el libro y en el DVD.

Aunque el apéndice es útil como herramienta de referencia, si tiene intención de convertir valores entre decimal y binario al realizar los diferentes tipos de problemas de subredes de los exámenes, en lugar de emplear los procesos abreviados que casi siempre evitan la aritmética binaria, posiblemente le resulte necesario practicar la conversión entre ambos formatos antes del examen. Para practicar, seleccione cualquier valor decimal entre 0 y 255, tradúzcalo a binario de 8 bits, y utilice después esta tabla para ver si ha obtenido la respuesta correcta. Además, seleccione cualquier número binario de 8 bits, tradúzcalo a decimal, y utilice de nuevo la tabla para comprobar los resultados.

Valor decimal	Valor binario	Valor decimal	Valor binario	Valor decimal	Valor binario	Valor decimal	Valor binario
0	00000000	32	00100000	64	01000000	96	01100000
1	00000001	33	00100001	65	01000001	97	01100001
2	00000010	34	00100010	66	01000010	98	01100010
3	00000011	35	00100011	67	01000011	99	01100011
4	00000100	36	00100100	68	01000100	100	01100100
5	00000101	37	00100101	69	01000101	101	01100101
6	00000110	38	00100110	70	01000110	102	01100110
7	00000111	39	00100111	71	01000111	103	01100111
8	00001000	40	00101000	72	01001000	104	01101000
9	00001001	41	00101001	73	01001001	105	01101001
10	00001010	42	00101010	74	01001010	106	01101010
11	00001011	43	00101011	75	01001011	107	01101011
12	00001100	44	00101100	76	01001100	108	01101100
13	00001101	45	00101101	77	01001101	109	01101101
14	00001110	46	00101110	78	01001110	110	01101110
15	00001111	47	00101111	79	01001111	111	01101111
16	00010000	48	00110000	80	01010000	112	01110000
17	00010001	49	00110001	81	01010001	113	01110001
18	00010010	50	00110010	82	01010010	114	01110010
19	00010011	51	00110011	83	01010011	115	01110011
20	00010100	52	00110100	84	01010100	116	01110100
21	00010101	53	00110101	85	01010101	117	01110101
22	00010110	54	00110110	86	01010110	118	01110110
23	00010111	55	00110111	87	01010111	119	01110111
24	00011000	56	00111000	88	01011000	120	01111000
25	00011001	57	00111001	89	01011001	121	01111001
26	00011010	58	00111010	90	01011010	122	01111010
27	00011011	59	00111011	91	01011011	123	01111011
28	00011100	60	00111100	92	01011100	124	01111100
29	00011101	61	00111101	93	01011101	125	01111101
30	00011110	62	00111110	94	01011110	126	01111110
31	00011111	63	00111111	95	01011111	127	01111111

Valor decimal	Valor binario	Valor decimal	Valor binario	Valor decimal	Valor binario	Valor decimal	Valor binario
128	10000000	160	10100000	192	11000000	224	11100000
129	10000001	161	10100001	193	11000001	225	11100001
130	10000010	162	10100010	194	11000010	226	11100010
131	10000011	163	10100011	195	11000011	227	11100011
132	10000100	164	10100100	196	11000100	228	11100100
133	10000101	165	10100101	197	11000101	229	11100101
134	10000110	166	10100110	198	11000110	230	11100110
135	10000111	167	10100111	199	11000111	231	11100111
136	10001000	168	10101000	200	11001000	232	11101000
137	10001001	169	10101001	201	11001001	233	11101001
138	10001010	170	10101010	202	11001010	234	11101010
139	10001011	171	10101011	203	11001011	235	11101011
140	10001100	172	10101100	204	11001100	236	11101100
141	10001101	173	10101101	205	11001101	237	11101101
142	10001110	174	10101110	206	11001110	238	11101110
143	10001111	175	10101111	207	11001111	239	11101111
144	10010000	176	10110000	208	11010000	240	11110000
145	10010001	177	10110001	209	11010001	241	11110001
146	10010010	178	10110010	210	11010010	242	11110010
147	10010011	179	10110011	211	11010011	243	11110011
148	10010100	180	10110100	212	11010100	244	11110100
149	10010101	181	10110101	213	11010101	245	11110101
150	10010110	182	10110110	214	11010110	246	11110110
151	10010111	183	10110111	215	11010111	247	11110111
152	10011000	184	10111000	216	11011000	248	11111000
153	10011001	185	10111001	217	11011001	249	11111001
154	10011010	186	10111010	218	11011010	250	11111010
155	10011011	187	10111011	219	11011011	251	11111011
156	10011100	188	10111100	220	11011100	252	11111100
157	10011101	189	10111101	221	11011101	253	11111101
158	10011110	190	10111110	222	11011110	254	11111110
159	10011111	191	10111111	223	11011111	255	11111111

cisco

APÉNDICE C

Actualizaciones del examen ICND2: Versión 1.0

Con el tiempo, la información facilitada por los lectores permite a Cisco calibrar qué temas suponen los mayores problemas a nuestros lectores cuando se presentan al examen. Además, Cisco puede hacer pequeños cambios en el alcance de los temas del examen, o puede hacer hincapié en ciertos temas. Para ayudar a nuestros lectores en ese sentido, el autor crea materiales nuevos que clarifican o explican los temas más difíciles a efectos del examen. Como se mencionaba en la introducción, el contenido adicional referente al examen está disponible en un documento PDF en el sitio web de este libro, en la dirección http://www.ciscopress.com/title/158720181x. El documento que está viendo es la versión 1.0 de este apéndice.

Este apéndice presenta la actualización más reciente que está disponible en el momento de imprimirse el libro. Para asegurarse de que dispone de la versión más reciente de este documento, no olvide visitar el sitio web del libro para ver si se han publicado versiones más recientes desde el momento en que el libro salió de la imprenta.

Este apéndice intenta llenar el vacío que se produce con cualquier libro que se imprime. En particular, este apéndice hace lo siguiente:

- Menciona datos técnicos que quizá no se hayan mencionado en otros lugares de libro.
- Trata temas nuevos cuando Cisco añade temas a las plantillas del examen ICND2 o CCNA.
- Proporciona una forma de obtener información muy reciente relativa al contenido de los exámenes.

Obtenga siempre lo más reciente en el sitio web

Lo que está leyendo es la versión de este apéndice que estaba disponible cuando se imprimió el libro. Sin embargo, como el propósito principal de este apéndice es ser un do-

cumento vivo y cambiante, es muy importante que busque la última versión online, en el sitio web del libro. Para hacer esto:

1. Vaya a la dirección http://www.ciscopress.com/title/158720181x.
2. Seleccione la opción Downloads que hay en el cuadro More Information.
3. Descárguese el documento "ICND2 Appendix C" más reciente.

Nota

Obsérvese que el documento descargado tiene un número de versión. Si la versión del PDF que hay en el sitio web es la misma que este apéndice del libro, el libro ya contiene la versión más reciente y no hay necesidad de descargar o utilizar la versión online.

Contenido técnico

La versión actual de este apéndice no contiene ningún tratamiento técnico adicional. Este apéndice esta aquí simplemente para ofrecer las instrucciones necesarias para comprobar en la Web si existe una versión posterior de este apéndice.

cisco

GLOSARIO

A

ABR. Router fronterizo (*Area Border Router*). Se trata de un router que emplea OSPF y que posee interfaces en varias áreas OSPF.

ACL. Lista de control de acceso (*Access Control List*). Es una lista que se configura en un router para controlar el flujo de paquetes a través del mismo, con objeto de evitar que los paquetes que tengan una determinada dirección IP salgan por una cierta interfaz del router.

ACL dinámica. Es un tipo de ACL que va más allá de las ACLs IP tradicionales, para permitir dinámicamente tráfico procedente de un host si previamente el host se conecta con el router vía Telnet y supera un proceso de autenticación.

ACL reflexiva. Es un tipo de ACL que va más allá de las ACLs IP tradicionales, y monitoriza las nuevas sesiones de usuario. El router reacciona para añadir una entrada de ACL que refleja la dirección IP de la sesión y sus números de puerto TCP y UDP.

Actualización activada (automática). Es una característica de los protocolos de enrutamiento consistente en que el protocolo no espera a la próxima actualización periódica cuando cambia algo en la red; en lugar de hacer esto, envía automáticamente una actualización de enrutamiento.

Actualización completa. Con los protocolos de enrutamiento IP, es el concepto general consistente en que una actualización del protocolo de enrutamiento contiene la lista de todas las rutas conocidas. Véase también Actualización parcial.

Actualización de estado del enlace (*link-state update*). Se trata de un paquete OSPF que sirve para enviar una LSA a un router vecino.

Actualización parcial. En los protocolos de enrutamiento IP, es un concepto general consistente en que una actualización del protocolo de enrutamiento sólo especifica un subconjunto de todas las rutas conocidas. Véase también Actualización completa.

Actualización periódica. En los protocolos de enrutamiento, concepto consistente en que el protocolo de enrutamiento publica las rutas de una actualización de enrutamiento de forma periódica y regular. Esto es típico de los protocolos de enrutamiento por vector de distancia.

Aislamiento de problemas. Es la parte del proceso de resolución de problemas en la cual el ingeniero intenta descartar posibles causas del problema, reduciendo el número de causas posibles hasta que sea posible identificar la causa principal o raíz del problema.

Algoritmo de actualización difuso. Véase DUAL.

Algoritmo SPF de Dijkstra. Primero la ruta más corta. Es el nombre del algoritmo que utilizan los protocolos de enrutamiento por estado del enlace para analizar la LSDB y buscar las rutas de coste mínimo desde ese router hasta cada subred.

AND. Es una operación matemática que se le aplica a una pareja de números binarios de un solo dígito. El resultado es otro número binario de un solo dígito. 1 AND 1 tiene el valor 1; todas las demás combinaciones producen el valor 0.

Aprender. Los puentes y los switches transparentes aprenden las direcciones MAC examinando las direcciones MAC de origen de las tramas que reciben. Van añadiendo a una tabla de direcciones las nuevas direcciones MAC, junto con el número de puerto del puerto a través del cual han aprendido esa dirección MAC.

Aprendizaje, estado. En STP, se trata de un estado temporal de los puertos, en el cual la interfaz no reenvía tramas, pero puede empezar a aprender direcciones MAC a partir de las tramas que se reciban en la interfaz.

AR. Velocidad de acceso. En Frame Relay, es la velocidad a la que se envían bits a través de un enlace de acceso.

ARP Inverso. (*Inverse ARP*) Es un protocolo de Frame Relay mediante el cual los routers publican su dirección de capa 3 a través de un CV, aportando de este modo a sus vecinos información útil de correspondencias entre la capa 3 y la capa 2.

ARP Protocolo de resolución de direcciones (*Address Resolution Protocol*). Es un protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC. Está definido en la RFC 826.

ASBR. Router límite de sistema autónomo (*Autonomous System Border Router*). Es un router que emplea OSPF, en el que el router aprende rutas a partir de otra fuente, normalmente otro protocolo de enrutamiento, intercambiando rutas que son externas a OSPF con el dominio OSPF.

Asignación de Frame Relay. Es la información que relaciona o asigna un DLCI de Frame Relay a la dirección de capa 3 del DTE que está en el otro extremo de un CV definido por el DLCI local.

Asíncrono. Describe una convención para el envío de datos mediante señales digitales. El emisor y el receptor operan a la misma velocidad, pero no se realiza esfuerzo alguno para conseguir dinámicamente que el emisor y el receptor ajusten sus velocidades basándose en la del otro dispositivo.

Autoconfiguración sin estado. Es una característica de IPv6 consistente en que se puede asignar una dirección de unidifusión de IPv6 a un host o a un router sin necesidad de un servidor DHCP con estado.

Autoresumen. Es una característica del protocolo de enrutamiento mediante la cual un router conectado a más de una red con clase publica las rutas resumidas para cada red con clase completa de redes con clase, cuando envía actualizaciones por las interfaces conectadas a otras redes con clase.

B

Base de datos de configuración de VLAN. Es el nombre de la configuración colectiva de IDs y nombres de VLAN en un switch Cisco.

Base de datos de estado del enlace (LSDB, *link-state database*). En OSPF, es la estructura de datos residente en la RAM de un router que contiene las distintas LSAs, donde las LSAs representan toda la topología de la red.

Base de datos topológica. Son los datos estructurados que describen la topología de la red a efectos de un protocolo de enrutamiento. Los protocolos de enrutamiento por estado del enlace e híbridos equilibrados emplean tablas topológicas, a partir de las cuales construyen las entradas de la tabla de enrutamiento.

Bc. Ráfaga comprometida (*committed burst*). Es un término de Frame Relay que se refiere al número de bits que se pueden enviar durante un intervalo de tiempo definido. Esto ayuda a determinar si/cuándo el DTE ha enviado a través de un CV, por término medio, más datos que lo que indica la velocidad definida en el contrato de tráfico.

BECN. Notificación de la congestión retrospectiva (*backward explicit congestion notification*). Es el bit de la cabecera de Frame Relay que implica que se está produciendo una congestión en la dirección opuesta a la de la trama (hacia atrás). Los switches y los DTEs pueden reaccionar reduciendo la velocidad a la que se envían datos en esa dirección.

Bloqueo, estado. En 802.1d STP, se trata del estado de un puerto en el cual no se procesan las tramas recibidas, y el switch no envía tramas a través de la interfaz, con la excepción de los mensajes STP.

BPDU. Unidad de datos del protocolo de puente (*bridge protocol data unit*). Es el nombre genérico que reciben los mensajes del Protocolo de árbol de extensión.

BPDU de saludo (hello). Es el mensaje de STP y RSTP que se emplea en la mayoría de las comunicaciones STP, que especifica el ID de puente del raíz, el ID de puente del dispositivo remitente y el coste del dispositivo remitente con el cual se puede alcanzar al dispositivo raíz.

BPDU Guard. Es una característica de los switches de Cisco, que está a la escucha de mensajes BDPU de STP, e inhabilita la interfaz si se recibe alguno. El objetivo es evitar bucles cuando se conecta un switch a un puerto al que se esperaba que sólo estuviera conectada una computadora.

BRI. Interfaz de acceso básico (*Basic Rate Interface*). Es una interfaz RDSI formada por dos canales de transporte y un canal de datos (D), destinada a la comunicación de circuito conmutado de voz, vídeo y datos.

C

Capa de *sockets* seguros (SSL, *Secure Sockets Layer*). Es un protocolo de seguridad integrado en los navegadores web más extendidos; ofrece servicios de codificación y autenticación entre el navegador y un sitio web.

CHAP. Protocolo de autenticación e intercambio de señales por desafío (*Challenge Handshake Authentication Protocol*). Es una característica de seguridad definida por PPP que permite que uno o los dos puntos finales de un enlace verifiquen la autenticidad del otro dispositivo como un dispositivo autorizado en particular.

CIDR. Herramienta estándar para asignar intervalos globales de direcciones IP. CIDR reduce el tamaño de las tablas de enrutamiento IP en los routers de Internet, y ayuda a paliar el rápido crecimiento de Internet. El término sin clase se refiere a que los grupos resumidos de redes representan un grupo de direcciones que no se ajustan a las reglas de agrupamiento con clase IPv4 (clases A, B o C).

CIDR, notación. Véase notación con prefijo.

CIR. Velocidad de información suscrita (*Committed Information Rate*). En Frame Relay y ATM, se trata de la velocidad media con que se pueden transmitir bits a lo largo de un circuito virtual según el contrato comercial existente entre el cliente y el proveedor de servicios.

Circuito virtual permanente (PVC). Se trata de una ruta de comunicaciones preconfigurada que existe entre dos DTEs Frame Relay, y está identificada mediante un DLCI en cada enlace de acceso Frame Relay; de este modo ofrece el equivalente funcional de un circuito alquilado, pero sin que haya una línea física alquilada para cada VC.

Clave compartida. Es una referencia a una clave de seguridad cuyo valor es conocido tanto por el remitente como por el destinatario.

Clave privada. Es un valor secreto que se utiliza en los sistemas de encriptación de clave pública y privada. O bien codifica un valor que después se puede decodificar empleando la clave pública correspondiente, o bien decodifica un valor que haya sido codificado previamente empleando la clave pública correspondiente.

Clave pública. Es un valor secreto que se utiliza en los sistemas de encriptación de clave pública y privada. O bien codifica un valor que después se podrá decodificar empleando la clave privada correspondiente, o bien decodifica un valor que ha sido codificado previamente con la clave privada correspondiente.

Cliente VPN. Es un programa que reside en un PC, normalmente en un portátil, de tal modo que esa computadora pueda implementar los protocolos necesarios para ser uno de los extremos de una VPN.

Codificación. Son las convenciones que indican la forma en que un dispositivo modifica unas señales eléctricas u ópticas que envía a través de un cable, para denotar un determinado código binario. Por ejemplo, un módem puede codificar un 1 o un 0 binario empleando una frecuencia para indicar un 1 y otra para indicar un 0.

Completamente adyacente. En OSPF, es una caracterización del estado de un vecino, consistente en que ambos vecinos han alcanzado el estado completo.

Condición de viabilidad. En EIGRP, cuando un router ha obtenido múltiples rutas para llegar a una subred, si la métrica de la mejor ruta es X, entonces la condición de viabilidad es otra ruta cuya distancia es <= X.

Conmutación de circuitos. Es el sistema conmutado en el que debe existir un circuito físico que una al emisor con el receptor mientras dure la "llamada". Se utiliza mucho en las redes de las compañías de telefonía.

Conmutación de paquetes. Se trata de un servicio WAN mediante el cual cada dispositivo DTE se conecta a una compañía de telefonía empleando una sola línea física, con la posibilidad de reenviar tráfico a todos los demás sitios que estén conectados al mismo ser-

vicio. El switch telefónico toma la decisión de reenviar basándose en una dirección que hay en la cabecera del paquete.

Convergencia. Es el tiempo necesario para que los protocolos de enrutamiento reaccionen frente a cambios en la red, descartando rutas incorrectas y añadiendo otras rutas nuevas y mejores, de tal modo que las mejores redes actuales consten en las tablas de enrutamiento de todos los routers.

CSU/DSU. Unidad de servicio de canal/unidad de servicio de datos (*Channel service unit/data service unit*). Se trata de un dispositivo que conecta un circuito físico instalado por la compañía de telefonía con algún dispositivo CPE, efectuando una adaptación entre las tensiones, corrientes, tramas y conectores que se utilizan en el circuito con la interfaz física que admita el DTE.

Cuenta hasta infinito. Es un lamentable efecto secundario de los protocolos de enrutamiento por vector de distancia, consistente en que los routers van incrementando lentamente la métrica de las rutas que fallan, hasta que el valor de la métrica alcanza la definición finita de máxima métrica para ese protocolo (que es lo que se llama infinito).

CV. Circuito virtual. Se trata de un concepto lógico que representa la ruta que siguen las tramas entre distintos DTEs. Los CVs son especialmente útiles cuando se compara la tecnología de Frame Relay con los circuitos físicos alquilados.

D

DCE. Equipo de comunicación de datos. Desde un punto de vista físico, el dispositivo que proporciona la sincronización en un enlace WAN, que normalmente es una CSU/DSU, es el DCE. Desde la perspectiva de la conmutación de paquetes, el switch del proveedor de servicios, al cual se podría conectar un router, es lo que se considera el DCE.

DCE Frame Relay. Es el switch Frame Relay.

DE. Posible para descarte (*discard eligible*). Se trata del bit presente en el encabezado de Frame Relay que, si es preciso descartar tramas, indica a los switches que descarten esa trama en lugar de otra en la que el bit DE no esté activado.

Denegado. Es la acción que lleva a cabo una ACL cuando ésta implica que hay que descartar un paquete.

Descarte, estado de. Se trata de un estado de interfaz RSTP en el que no se procesan las tramas recibidas, y el switch no retransmite tramas a través de la interfaz, con la excepción de mensajes RSTP.

Descripción de base de datos. Es un tipo de paquete OSPF que enumera breves descripciones de las LSA presentes en la LSDB de OSPF.

DHCP con estado. Es un término que se utiliza en IPv6 para diferenciarlo de DHCP sin estado. El mecanismo de DHCP con estado lleva la cuenta de los clientes a los que se ha asignado una dirección IP (información de estado).

DHCP sin estado. Es un término que se utiliza en IPv6 para diferenciarlo de DHCP con estado. Los servidores DHCP sin estado no alquilan temporalmente direcciones IPv6 a los

clientes. En su lugar, les proporcionan otra información útil, como las direcciones IP de los servidores DNS, pero sin necesidad de rastrear información relativa a los clientes (información de estado).

Dirección de difusión. Véase dirección de difusión de subred.

Dirección de difusión de subred. Es una dirección especial de cada subred; concretamente, la mayor dirección numérica de la subred, y está destinada a que los paquetes enviados a ella sean entregados a todos los hosts de la subred.

Dirección de difusión dirigida. Equivale al término dirección de difusión de subred.

Dirección de unidifusión global. Es un tipo de dirección IPv6 de unidifusión que se ha seleccionado dentro de un intervalo de direcciones IP públicas y globalmente exclusivas, según consta en los registros de ICANN, sus agencias subsidiarias y cualesquiera otros registros o proveedores de servicios.

Dirección IP secundaria. Es la segunda dirección IP (o más) que se configura en una interfaz de un router, empleando la palabra reservada `secondary` en el comando `ip address`.

Dirección local de un enlace. Es un tipo de dirección IPv6 de unidifusión que representa una interfaz de un único enlace de datos. Los paquetes que se envían a la dirección local de un enlace sólo atraviesan ese enlace concreto y nunca son enviados a otras subredes por algún router. Se utiliza para las comunicaciones que no necesitan abandonar el enlace local, como puede ser el descubrimiento de vecinos.

Dirección local exclusiva o única. Es un tipo de dirección de unidifusión IPv6 que se ha creado como sustituto de las direcciones privadas de IPv4.

Dirección privada. Se refiere a varias redes de clase A, B y C que se reservan para el uso dentro de organizaciones privadas. Estas direcciones, según lo definido en la RFC 1918, no se pueden enrutar a través de Internet.

Direccionamiento con clase. Es un concepto de direccionamiento propio de IPv4, que define las direcciones IP de subred como objetos formados por tres partes: red, subred y host.

Distancia administrativa. En los routers de Cisco, se trata de un medio empleado para optar por una de entre varias rutas para llegar a una misma subred, cuando esas rutas se han aprendido mediante distintos protocolos de enrutamiento. Cuanto menor es la distancia administrativa, más preferible es el origen de esa información de enrutamiento.

Distancia factible. En EIGRP, es la métrica de la mejor ruta para alcanzar una subred.

Distancia notificada o informada. Desde el punto de vista de un router EIGRP, es la métrica de una subred tal como se calcula en un router vecino, para después ser notificada al primer router mediante una actualización de enrutamiento.

DLCI. Identificador de conexión de enlace de datos (*Data-Link Connection Identifier*). Es la dirección de Frame Relay que identifica a un VC en un determinado enlace de acceso.

Dominio de difusión. Conjunto formado por todos los dispositivos que reciben tramas difundidas procedentes de cualquier dispositivo del conjunto. Los dispositivos que pertenecen a una misma VLAN se encuentran en un mismo dominio de difusión.

DTE. Equipo terminal de datos (*Data terminal equipment*). Desde la perspectiva de la capa 1, el DTE sincroniza su reloj basándose en el pulso enviado por el DCE. Desde la pers-

pectiva de la conmutación de paquetes, el DTE es el dispositivo que está fuera de la red del proveedor de servicios, y normalmente es un router.

DTE Frame Relay. Es el dispositivo cliente que está conectado a un enlace de acceso Frame Relay; normalmente es un router.

DUAL. Algoritmo de actualización difuso (*Diffusing Update Algorithm*). Es un algoritmo de convergencia que se emplea en EIGRP cuando falla una ruta y el router no dispone de una ruta sustitutiva factible. DUAL hace que los routers envíen mensajes EIGRP de tipo "petición y respuesta" para descubrir rutas alternativas que no contengan bucles.

E

EIGRP. Protocolo de enrutamiento de gateway interior mejorado (*Enhanced Interior Gateway Routing Protocol*). Es una versión avanzada de IGRP desarrollada por Cisco. Ofrece mejores características de convergencia y de eficiencia operativa, y combina las ventajas de los protocolos por estado del enlace con las de los protocolos por vector de distancia.

Enlace de acceso. En Frame Relay, es el enlace físico en serie que conecta un DTE de Frame Relay, que normalmente será un router, con un switch de Frame Relay. Los enlaces de acceso emplean los mismos estándares de capa física que las líneas punto a punto alquiladas.

Enlace entre switches. Véase ISL.

Enrutamiento con clase. Es una variación del proceso de envío (enrutamiento) de IPv4 que define los detalles de cómo se utiliza la ruta predeterminada. La ruta predeterminada solamente se usa si la red con clase en la que reside la dirección de destino del paquete no se encuentra en la tabla de enrutamiento del router.

Enrutamiento entre dominios sin clase. Véase CIDR.

Enrutamiento sin clase. Es una variante del proceso de envío (enrutamiento) de IPv4 que define las peculiaridades de la forma en que se utiliza la ruta predeterminada. Esta última siempre es útil para aquellos paquetes cuya dirección IP de destino no coincide con ninguna otra ruta.

Enrutamiento sin clase. Se trata de un concepto de direccionamiento IPv4 que establece que las direcciones IP de subred poseen dos partes: un prefijo (o subred) y un host.

Entramado. Son las convenciones que especifican la forma en que la capa 2 interpreta los bits que se envían de acuerdo con la capa 1 de ISA. Por ejemplo, cuando se ha recibido una señal eléctrica y se ha convertido esa señal a binario, el entramado identifica los campos de información que hay dentro de los datos.

Enviar. Enviar una trama hacia su destino final a través de algún dispositivo de red.

Envío, estado. Se trata del estado de un puerto STP y RSTP en el cual la interfaz funciona sin verse restringida por STP.

Escucha, estado. Se trata de un estado temporal en puertos STP que se produce inmediatamente después de que una interfaz pase de estar en modo de bloqueo a estar en modo de reenvío. Durante este estado, el switch invalida las entradas de las tablas MAC. Tam-

bién ignora las tramas recibidas en la interfaz, y no reenvía trama alguna a través de la interfaz.

Estado bidireccional. En OSPF, se trata del estado de vecindad que implica que el router ha intercambiado mensajes de saludo (hellos) con el vecino, y que se satisfacen todos los parámetros requeridos.

Estado completado. (*full state*) En OSPF, denota el estado de un vecino que implica que los dos routers han intercambiado todo el contenido de sus respectivas LSDBs.

Estado del enlace. Es una clasificación del algoritmo subyacente que se emplea en algunos protocolos de enrutamiento. Los protocolos por estado del enlace construyen una detallada base de datos que especifica los enlaces (subredes) y su estado (activo, inactivo), a partir de la cual se pueden calcular las mejores rutas.

EtherChannel. Es una característica exclusiva de Cisco, consistente en que es posible combinar hasta ocho segmentos Ethernet paralelos entre dos dispositivos concretos, todos ellos operando a la misma velocidad, para que actúen como un único enlace para reenviar paquetes y emplear la lógica del Protocolo de árbol de extensión.

Externa global. Es un término de NAT que se refiere a una dirección IP que se emplea para un host situado en la parte externa (no de confianza) de la red; es la dirección que se usa en los paquetes cuando estos recorren la parte externa de la red, que normalmente es la Internet global.

Externa local. Es un término de NAT que se refiere a una dirección IP que se emplea para un host situado en la parte externa (no de confianza) de la red; es la dirección que se usa en los paquetes cuando estos recorren la parte interna de la red (la de confianza) o parte local.

F

FECN. Notificación explícita de la congestión (*forward explicit congestion notification*). Se trata del bit del encabezado de Frame Relay que indica a cualquiera que reciba esa trama (los switches y los DTEs) que se está produciendo una congestión en la misma dirección que la trama.

Filtro. En general, se trata de un proceso o dispositivo que estudia el tráfico de red en busca de ciertas características, tales como una dirección de origen, una dirección de destino o un protocolo. Este proceso determina si debe enviarse o descartarse ese tráfico basándose en los criterios establecidos.

Frame Relay. Se trata de un protocolo de enlace de datos estándar internacional, que define las capacidades que debe tener un servicio de conmutación de tramas (o conmutación de paquetes), y que permite a los dispositivos DTE (que normalmente son routers) enviar datos a muchos otros dispositivos, empleando una sola conexión física con el servicio Frame Relay.

FTP. Protocolo de transferencia de archivos (*File Transfer Protocol*). Es un protocolo de aplicación, que forma parte del conjunto de protocolos TCP/IP, y que sirve para transmitir archivos entre los nodos de una red. FTP está definido en la RFC 959.

Full duplex. De forma genérica, se refiere a cualquier comunicación en la que los dos dispositivos implicados pueden enviar y recibir datos de manera concurrente. Para las LANs Ethernet, significa específicamente que ambos dispositivos tienen la capacidad de enviar y recibir al mismo tiempo. Esto sólo se permite cuando nada más hay dos estaciones en un dominio de colisión. La comunicación full duplex se habilita desactivando la lógica de detección de colisiones CSMA/CD.

H

HDLC. Control de enlace de datos de capa superior (*High-Level Data-Link Control*). Se trata de un protocolo de la capa de enlace de datos, síncrono y orientado a bits, que ha sido desarrollado por la Organización internacional para la normalización (ISO, *Organization for Standardization*). Derivado del Control de enlace de datos síncrono (SDLC), HDLC especifica un método para el encapsulamiento de datos en enlaces serie síncronos, empleando caracteres de trama y sumas de comprobación.

Hello. Véase Saludo.

Hello inferior. Véase Saludo inferior.

Hello, temporizador. Véase Saludo, temporizador.

Híbrido equilibrado. Se refiere a uno de los tres tipos generales de algoritmos de los protocolos de enrutamiento. Los otros dos son el vector de distancia y el estado del enlace. EIGRP es el único protocolo de enrutamiento que Cisco considera que utiliza un algoritmo híbrido equilibrado.

Holddown. Se trata de un estado del protocolo por vector de distancia que se asigna a ciertas rutas para que los routers no publiquen su disponibilidad ni acepten publicaciones de que está disponible durante un cierto período de tiempo (que es el que indica el temporizador *holddown*). Este estado se emplea para descartar informaciones incorrectas sobre una cierta ruta en todos los routers de la red. Normalmente, se rechaza una ruta cuando hay un enlace de esa ruta que falla.

Horizonte dividido. Es una técnica de enrutamiento por vector de distancia en la cual la información sobre rutas no puede salir por la misma interfaz del router a través de la que se ha recibido. Las actualizaciones de horizonte dividido son útiles para evitar los bucles de enrutamiento.

I

ID de puente (BID). Es un identificador de 8 bytes para puentes y switches, que se emplea en STP y RSTP. Consta de un campo de prioridad de 2 bytes, seguido por un campo de identificación de sistema de 6 bytes que normalmente se rellena con una dirección MAC.

ID de router (RID). En OSPF, es un número de 32 bits, escrito en decimal con puntos, que identifica de forma exclusiva a cada router.

Identificador de conexión de enlace de datos. Véase DLCI.

IEEE 802.11. Es el estándar básico del IEEE para las LANs inalámbricas.

IEEE 802.1ad. Es el estándar del IEEE para el equivalente funcional de EtherChannel, que es propiedad de Cisco.

IEEE 802.1d. Es el estándar del IEEE correspondiente al Protocolo de árbol de extensión original.

IEEE 802.1Q. Es el protocolo de *trunking* VLAN según el estándar del IEEE. El 802.1Q incluye el concepto de una VLAN nativa, para la cual no se añade un encabezado de VLAN, y se inserta un encabezado de VLAN después del campo original de tipo/longitud.

IEEE 802.1s. Es el estándar del IEEE para Múltiples instancias del árbol de extensión (MIST, *Multiple Instances of Spanning Tree*), que permite equilibrar las cargas de tráficos entre distintas VLANs.

IEEE 802.1w. Es el estándar del IEEE para una versión mejorada de STP, denominada STP rápido, que acelera la convergencia.

IEEE 802.3. Es el estándar base del IEEE para las LAN similares a Ethernet.

IGRP. Protocolo de enrutamiento de gateway interior (*Interior Gateway Routing Protocol*). Es un protocolo de gateway interior (IGP, *Interior Gateway Protocol*) antiguo y que ya no se utiliza; fue desarrollado por Cisco.

Infinito. En el contexto de los protocolos de enrutamiento IP, se trata de un valor finito de métrica, definido por el protocolo de enrutamiento, que se emplea para denotar una ruta no utilizable en una actualización del protocolo de enrutamiento.

Intercambio de claves Diffie-Hellman. Se trata de un protocolo de intercambio de claves mediante el cual dos dispositivos pueden intercambiar información a través de una red pública. En combinación con ciertos secretos ya existentes permite calcular una clave simétrica que sólo ellos conocen.

Interfaz de administración local (LMI, *Local Management Interface*). Se trata de un protocolo de Frame Relay que se emplea entre un DTE (router) y un DCE (switch Frame Relay). La LMI actúa como mecanismo *keepalive*. La ausencia de mensajes LMI indica que ha fallado el otro dispositivo. También indica al DTE la existencia de todos los CVs y DLCIs, junto con su estado.

Interna global. Es un término de NAT que se refiere a la dirección IP que se emplea para un host situado dentro de la parte de confianza de la red, pero en paquetes que recorren la parte global (que no es de confianza) de la red.

Interna local. Es un término de NAT que se refiere a la dirección IP que se utiliza para un host que se halla dentro de la parte de confianza de la red, pero en paquetes que recorren la parte local (de confianza) de la red.

Intervalo hello. Véase Saludo, intervalo de.

Inversa envenenada. Es una publicación de una ruta envenenada por vector de distancia correspondiente a una subred que no habría constado en la publicación por las reglas de horizonte dividido, pero que ahora se incluye en la publicación como ruta envenenada.

IPCP. Protocolo de control IP (*IP Control Protocol*). Se trata de un protocolo de control que se define dentro de PPP con el propósito de inicializar y controlar el envío de paquetes IPv4 a través de un enlace PPP.

IPsec. Es un término que se refiere a los protocolos de seguridad IP, que forman una arquitectura para proporcionar servicios de encriptación y autenticación, normalmente cuando se están creando servicios VPN a través de una red IP.

ISL. Enlace entre switches (*Inter-Switch Link*). Es el protocolo de *trunking* VLAN exclusivo de Cisco que se adelantó muchos años al 802.1Q. ISL define un encabezado de 26 bytes que encapsula una trama original de Ethernet.

K

Keepalive. Es una característica de muchos protocolos de enlace de datos consistente en que el router envía periódicamente mensajes al router vecino para hacerle saber que todavía se encuentra operativo y en perfectas condiciones.

L

LAN virtual (VLAN). Es un grupo de dispositivos conectados a uno o más switches que se agrupan en un solo dominio de difusión mediante una configuración. Las VLANs permiten a los administradores de switches ubicar los dispositivos conectados a los switches en distintas VLANs sin que se necesiten switches físicamente distintos. Esto produce ventajas de diseño, separando el tráfico sin el gasto que supone comprar hardware adicional.

LAPF. Define la cabecera y la información final básicas de Frame Relay. La cabecera incluye los bits DLCI, FECN, BECN y DE.

Línea alquilada. Es una línea de transmisión reservada por un proveedor de comunicaciones para el uso privado de un cliente. Las líneas alquiladas son normalmente líneas dedicadas.

Lista de acceso con nombre. Es una ACL que identifica las distintas sentencias de la ACL basándose en un nombre, en lugar de emplear un número.

Lista de acceso estándar. Es una lista de comandos de configuración global del IOS que sólo pueden coincidir con la dirección IP de un paquete, con el propósito de decidir qué paquetes se van a descartar y cuáles podrán atravesar el router.

Lista de acceso extendida. Es una lista de comandos de configuración global access-list del IOS para listas de acceso que puede denotar múltiples partes de un paquete IP, incluyendo la dirección IP de origen y de destino y los puertos TCP/UDP, con el propósito de decidir qué paquetes se van a descartar y cuáles podrán pasar a través del router.

LSA. Publicación de estado del enlace (*Link State Advertisement*). En OSPF, se trata del nombre de la estructura de datos que reside dentro de la LSDB y que describe detalladamente los distintos componentes de la red, incluyendo los routers y los enlaces (las subredes).

M

Malla parcial. Se trata de una topología de red en la cual hay más de dos dispositivos que podrían comunicarse físicamente; sin embargo, por decisión propia, sólo se permite que un cierto subconjunto de las parejas de dispositivos que están conectados a la red puedan comunicarse directamente.

Máscara. Véase máscara de subred.

Máscara de subred. Es un número de 32 bits que describe el formato de una dirección IP. Representa los bits de red y subred combinados que hay en la dirección con los valores de bit de la máscara iguales a 1, y los bits de host de la dirección con los valores de bit de la máscara iguales a 0.

Máscara de subred de longitud variable. Véase VLSM.

Máscara *wildcard*. Es la máscara que se utiliza en los comandos IOS de las ACLs de Cisco, y en los comandos network de OSPF y de EIGRP.

MaxAge. En STP, se trata de un temporizador que indica cuánto tiempo debe esperar un switch cuando ya no recibe mensajes de saludo procedentes del switch raíz antes de actuar para hacer que vuelva a converger la topología STP. También se denomina temporizador de edad máxima.

Métrica. Es una medida numérica que emplean los protocolos de enrutamiento para determinar hasta qué punto es buena una ruta en comparación con otras rutas alternativas para llegar a una misma subred.

MLP. Protocolo multienlace punto a punto (*Multilink Point-to-Point Protocol*). Se trata de un método para fragmentar, reensamblar y secuenciar tramas entre múltiples enlaces WAN punto a punto.

Modo administrativo de *trunking*. Son los ajustes de configuración del *trunking* de una interfaz en un switch de Cisco, tal como se hayan establecido mediante el comando switchport mode.

Modo administrativo. Véase Modo administrativo de *trunking*.

Modo de cliente VTP. Es uno de los tres modos operacionales de VTP en un switch; en este modo los switches pueden averiguar los números y nombres de otras VLANs a partir de otros switches, pero no se permite al switch que se pueda configurar directamente con información de la VLAN.

Modo operativo de *trunking*. Es el comportamiento actual de una interfaz de los switches Cisco para el *trunking* VLAN.

Modo servidor VTP. Es uno de los conjuntos de características de funcionamiento (modos) de VTP. Los switches que están en modo servidor pueden configurar VLANs, notificar los cambios a otros switches y aprender la existencia de cambios en la VLAN a partir de otros switches.

Modo transparente VTP. Es uno de los tres conjuntos de características de funcionamiento (modos) de VTP. Los switches que están en modo transparente pueden configurar VLANs, pero no comunican los cambios a otros switches, y tampoco aprenden la existencia de cambios en la VLAN a partir de otros switches.

MTU. Unidad máxima de transmisión (*Maximum transmission unit*). Es el tamaño máximo del paquete, medido en bytes, que puede admitir una determinada interfaz.

Muerto, temporizador. En OSPF, es un temporizador que se utiliza para todos y cada uno de los vecinos. El router considera que un vecino ha fallado si no se recibe ningún Saludo (Hello) de ese vecino en el intervalo de tiempo definido por el temporizador.

Multiacceso sin difusión (*nonbroadcast multiaccess*). Se trata de una caracterización de un cierto tipo de red de la capa 2 en la que dos dispositivos se conectan a la red, pero la red no permite que las tramas transmitidas se envíen a todos los dispositivos de la red.

N

NAT. Conversión de direcciones de red (*Network Address Translation*). Se trata de un mecanismo para reducir la necesidad de direcciones IPv4 que sean globalmente exclusivas. El mecanismo NAT permite a una organización con direcciones que no son globalmente exclusivas conectarse a Internet, convirtiendo esas direcciones al espacio de direcciones enrutables globalmente.

NAT, sobrecarga. Véase Conversión de direcciones de puerto (PAT, *Port Address Translation*).

NAT-PT. Es una característica de IPv6 consistente en que se traducen paquetes entre IPv4 e IPv6.

NBMA. Véase Multiacceso sin difusión.

Notación con prefijo. Es una forma abreviada de escribir una máscara de subred en la cual el número de unos binarios que hay en la máscara se escribe simplemente en decimal. Por ejemplo, /24 denota la máscara de subred que posee 24 unos binarios en la máscara de subred. Se considera que el número de bits cuyo valor binario es 1 es el prefijo.

O

OSPF. Primero la ruta libre más corta (*Open Shortest Path First*). Se trata de un popular IGP por estado del enlace que utiliza una base de datos formada por los estados de los enlaces y el algoritmo SPF para calcular las mejores rutas con objeto de llegar a todas las subredes conocidas.

P

PAP. Protocolo de autenticación de contraseña (*Password Authentication Protocol*). Es un protocolo PPP de autenticación que permite a los pares PPP autenticarse entre sí.

PAT. Conversión de direcciones de puerto (*Port Address Translation*). Es una característica de NAT consistente en que una dirección IP global interna admite más de 65000 conexiones TCP y UDP concurrentes.

Permiso. Es una acción que se lleva a cabo mediante una ACL y que implica que se consiente que un paquete pase por el router y sea reenviado.

Pila dual. En IPv6, es un modo de funcionamiento en el cual hay una computadora o un router en el que operan tanto IPv4 como IPv6.

ping extendido. Es un comando del IOS en el que el comando ping acepta muchas otras opciones además de la dirección IP de destino.

PortFast. Es una característica de la conmutación STP mediante la cual se sitúa un puerto en un estado de reenvío STP en cuanto se activa la interfaz, ignorando los estados de escucha y aprendizaje. Esta característica está destinada a puertos conectados a dispositivos de usuarios finales.

PPP. Protocolo punto a punto (*Point-to-Point Protocol*). Es un protocolo de enlace de datos que proporciona conexiones entre routers y entre hosts y redes, empleando para ellos circuitos síncronos y asíncronos.

Prefijo de registro. En IPv6, es el prefijo que describe un bloque de direcciones IPv6 públicas y globalmente exclusivas y que le han sido asignadas a un Registro regional de Internet por parte de la ICANN.

Prefijo de sitio. En IPv6, es el prefijo que describe un bloque de direcciones IPv6 globalmente exclusivas que le ha sido otorgado a una organización de usuarios finales (por ejemplo, a una empresa o agencia gubernamental). Normalmente, la asignación la realiza un ISP o un registro de Internet.

Prefijo de subred. En IPv6, es un término que denota el prefijo que se le asigna a cada enlace de datos, y actúa como una subred en IPv4.

Prefijo ISP. En IPv6, es el prefijo que describe un bloque de direcciones que le ha sido asignado a un ISP por parte de algún registro de Internet.

PRI. Interfaz de acceso principal (*Primary Rate Interface*). Es una interfaz RDSI con una velocidad de acceso básica. La velocidad de acceso básica consiste en un único canal D de 64 kbps, más 23 canales T1 o 30 canales E1 de tipo B para voz o datos.

Protocolo de árbol de extensión (STP, *Spanning Tree Protocol*). Es un protocolo definido por el estándar 802.1d del IEEE. Permite a los switches y puentes crear una LAN redundante, en la que el protocolo dará lugar dinámicamente a que ciertos puertos bloqueen el tráfico, para que la lógica de reenvío de los puentes y switches no dé lugar a que las tramas efectúen bucles indefinidamente dentro de la LAN.

Protocolo de árbol de extensión rápido (RSTP, *Rapid Spanning Tree Protocol*). Está definido por el IEEE 802.1w. Define una versión mejorada de STP que converge de manera mucho más rápida y segura que STP (802.1d).

Protocolo de control de enlace. (*Link Control Protocol*) Es un protocolo de control que se define dentro de PPP con el propósito de inicializar y mantener un enlace PPP.

Protocolo de descubrimiento de vecinos (NDP, *Neighbor Discovery Protocol*). Se trata de un protocolo que forma parte del conjunto de protocolos IPv6, y sirve para descubrir e intercambiar información relativa a dispositivos de la misma subred (los vecinos). En particular, sustituye al protocolo ARP de IPv4.

Protocolo de enrutamiento. Es un conjunto de mensajes y procesos mediante los cuales los routers pueden intercambiar información relativa a rutas para llegar a las subredes

de una determinada red. Entre los ejemplos de protocolos de enrutamiento se cuentan EIGRP, OSPF y RIP.

Protocolo de enrutamiento con clase. Se trata de una característica inherente de los protocolos de enrutamiento. Específicamente, el protocolo de enrutamiento no envía máscaras de subred en sus actualizaciones de enrutamiento. Esto requiere que el protocolo haga suposiciones relativas a las redes con clase y hace que no pueda admitir VLSM ni los resúmenes manuales de rutas.

Protocolo de enrutamiento sin clase. Es una característica inherente de los protocolos de enrutamiento. Específicamente, el protocolo de enrutamiento envía máscaras de subred en sus actualizaciones de enrutamiento, y de este modo descarta toda necesidad de hacer suposiciones relativas a las direcciones de una determinada red o subred. Esto hace posible que el protocolo admita VLSM y el resumen manual de rutas.

Protocolo de gateway exterior. EGP (*exterior gateway protocol*). Es un protocolo de enrutamiento destinado al intercambio de información entre distintos sistemas autónomos.

Protocolo de gateway interior. (IGP, *interior gateway protocol*) Es un protocolo enrutamiento que sirve para intercambiar información de enrutamiento dentro de un único sistema autónomo.

Protocolo de *trunking* VLAN (VTP). Es un protocolo de mensajería exclusivo de Cisco, que se emplea entre switches Cisco para comunicar información de configuración relativa a la existencia de distintas VLANs, incluyendo el ID y el nombre de la VLAN.

Protocolo enrutable. Véase Protocolo enrutado.

Protocolo enrutado. Es un protocolo de capa 3 que define paquetes que se pueden enrutar, como IPv4 e IPv6.

***Pruning* VTP.** Es la característica de VTP consistente en que los switches seleccionan dinámicamente las interfaces en las cuales hay que evitar la inundación de tramas en ciertas VLANs cuando las tramas no necesitan llegar a todos los switches de la red.

Publicación de estado del enlace. Véase LSA.

Puente raíz. Véase Switch raíz.

Puerto. (múltiples definiciones) 1) En TCP y UDP, es un número que sirve para identificar de forma exclusiva al proceso de aplicación que ha enviado (puerto de origen) o debería recibir (puerto de destino) los datos. 2) En conmutación LAN, es otro término que denota la interfaz de un switch.

Puerto alternativo. En RSTP 802.1w, denota un rol de puerto que se emplea para identificar una interfaz que está recibiendo una BPDU Hello inferior, lo que la convierte en posible sustituta del puerto raíz. También se utiliza en la implementación de STP 802.1d de Cisco.

Puerto de respaldo. En RSTP 802.1w, es un rol de puerto que se emplea cuando hay varias interfaces de un switch que se conectan a un único dominio de colisión. Esto hace que una de las interfaces sea el puerto designado (PD), y que una o más de las otras pasen a estar disponibles para sustituir al PD (rol de respaldo).

Puerto designado (DP). Tanto en STP como en RSTP, se trata de un rol de puerto que sirve para determinar cuál de las múltiples interfaces conectadas a un mismo segmento o

dominio de colisión debe emplearse para reenviar tramas al segmento. El switch que ofrezca la BDPU de saludo con coste mínimo pasa a ser el DP.

Puerto inhabilitado. En STP, es un rol de puerto para interfaces no operativas; en otras palabras, para interfaces que no se encuentran en un estado de conexión o *up/up*.

Puerto raíz. En STP, es el único puerto de un switch no raíz por el cual se recibe el Saludo de coste mínimo. Los switches ponen los puertos raíz en el estado de envío.

PVC. Véase Circuito virtual permanente.

R

RDSI. Red digital de servicios integrados (ISDN, *Integrated Services Digital Network*). Se trata de un protocolo de comunicación que ofrecen las compañías de telefonía y que permite a las redes telefónicas transportar datos, voz y vídeo.

Red con clase. Una red IPv4 de clase A, B o C. Se llaman redes con clase porque estas redes están definidas mediante las reglas de clases que especifica el direccionamiento IPv4.

Red contigua. En IPv4, es un diseño de red en el cual los paquetes que se retransmiten entre dos subredes de una única red con clase pasan únicamente a través de las subredes de la red con clase.

Red IP privada. Es uno de entre varios números de red IPv4 con clase que nunca se reservará para su uso en Internet; está destinado a ser utilizado dentro de una sola empresa.

Red privada virtual (VPN). Es un conjunto de protocolos de seguridad que, cuando se implementan en dos dispositivos situados a ambos lados de una red insegura tal como Internet, pueden permitir a los dispositivos enviar datos de forma segura. Las VPNs ofrecen un funcionamiento privado, autenticación de dispositivos, servicios que impiden la duplicación, y servicios de integridad de datos.

Red separada o disconinua. En IPv4, se trata de un diseño de red en el cual los paquetes que se reenvían entre dos subredes de una misma red con clase tienen que pasar a través de las subredes de otra red con clase.

Registro regional de Internet (RIR, *Regional Internet Registry*). Es el término genérico que denota una de las cinco organizaciones actuales que tienen la responsabilidad de repartir el espacio global y exclusivo de direcciones IPv4 e IPv6.

Resumen de rutas. Es el proceso consistente en combinar varias rutas en una sola ruta notificada, con objeto de reducir el número de entradas que hay en la tabla de enrutamiento IP del router.

Retardo de envío. Es un temporizador de STP, que de forma predeterminada dura 15 segundos, y sirve para especificar la cantidad de tiempo que permanece una interfaz en los estados de escucha y aprendizaje. También se llama temporizador de retardo de envío.

RIP. Protocolo de información de enrutamiento (*Routing Information Protocol*). Es un protocolo de gateway interior (IGP) que emplea la lógica por vector de distancia y una cuenta de saltos de router a router como métrica. La versión 1 de RIP (RIP-1) se ha vuelto impopular. La versión 2 de RIP (RIP-2) ofrece más posibilidades, incluyendo el soporte de VLSM.

Router designado. En OSPF, en redes multiacceso, se trata del router que gana unas elecciones y, por tanto, es el responsable de administrar un proceso optimizado para intercambiar información sobre la topología de OSPF con todos los routers conectados a esa red.

Router designado de respaldo. Es un router OSPF que está conectado a una red multiacceso, que monitoriza el funcionamiento del router designado (ED), y que asume la tarea del ED si éste falla.

Router fronterizo. Véase ABR.

Router límite de sistema autónomo. Véase ASBR.

RSTP. Véase Protocolo de árbol de extensión rápido.

Ruta envenenada. Una ruta de la publicación de un protocolo de enrutamiento que contiene una subred dotada de un valor de métrica especial, llamado métrica infinita; este valor indica que la ruta ha fallado.

Ruta hacia adelante. Desde la perspectiva de un host, es la ruta a través de la cual viaja un paquete en dirección a algún otro punto.

Ruta inversa. Desde la perspectiva de un host, y para los paquetes que se devuelven a ese host desde otro, se trata de la ruta a través de la que viaja el paquete.

Ruta resumida. Es una ruta que se crea mediante comandos de configuración para representar rutas que van a una o más subredes mediante una sola ruta, reduciendo de este modo el tamaño de la tabla de enrutamiento.

S

Saludo (hello). (Múltiples definiciones) 1) Protocolo que emplean los routers OSPF para descubrir, establecer y mantener relaciones con sus vecinos. 2) Protocolo que utilizan los routers EIGRP para descubrir, establecer y mantener relaciones con sus vecinos. 3) En STP, se refiere al nombre del mensaje periódico que envía el puente raíz en un árbol de extensión

Saludo inferior. Cuando se comparan dos o más BDPUs de saludo que se han recibido, se trata de un saludo con un ID de puente numéricamente mayor que el de otro saludo, o bien de un saludo que especifica el mismo ID de puente raíz, pero con un coste mayor.

Saludo, intervalo de. Con OSPF y EIGRP, es un temporizador de interfaz que determina la frecuencia con que la interfaz debe enviar mensajes de Saludo.

Saludo, temporizador. En STP, es el intervalo de tiempo transcurrido el cual el switch raíz debe enviar las BPDUs de Saludo.

Segmento. (Varias definiciones) 1) En TCP, es un término que se utiliza para describir un encabezado TCP y los datos encapsulados (también se denomina L4PDU). 2) También en TCP, es el conjunto de bytes que se forman cuando TCP fragmenta un gran bloque de datos que le proporciona la capa de aplicación en trozos menores, que caben en segmentos TCP. 3) En Ethernet, puede ser un cierto cable Ethernet o un cierto dominio de colisión (independientemente del número de cables que se utilicen).

Síncrono. Es la imposición de un orden temporal en un flujo de bits. En la práctica, un dispositivo intenta emplear la misma velocidad que otro dispositivo que se encuentra al otro extremo de un enlace serie. Sin embargo, si se examinan las transiciones entre estados de voltaje del enlace, el dispositivo puede apreciar ligeras variaciones de velocidad en ambos extremos, y ajustar su velocidad en consecuencia.

SLSM. Máscara de subred de longitud estática (*Static-length subnet mask*). Denota la utilización de la misma máscara de subred para todas las subredes de una sola red de clase A, B o C.

Solicitud de estado del enlace (*link-state request*). Se trata de un paquete OSPF que sirve para pedir a un router vecino que envíe una determinada LSA.

SSL. Véase Capa de *sockets* seguros.

Subinterfaz. Es una de las interfaces virtuales de una única interfaz física.

Subred. Es una subdivisión de una red de clase A, B o C, tal como la haya configurado el administrador de la red. Las subredes permiten utilizar una sola red de clase A, B o C, y siguen admitiendo un elevado número de grupos de direcciones IP, tal como se requiere para un enrutamiento IP eficaz.

Subred cero. Para toda red IPv4 con clase dividida en subredes, se trata de la subred cuyo número de subred tiene todos los dígitos binarios de la parte de subred del número a 0. En decimal, la subred 0 se puede identificar fácilmente porque es el mismo número que el número de red con clase.

Subred de difusión. Cuando se crea una subred en una red de clase A, B o C, alude a la única subred de cada red con clase para la cual todos los bits de subred tienen un valor binario de 1. La dirección de difusión de subred de esta subred tiene el mismo valor numérico que la dirección global de difusión de la red con clase.

Subredes superpuestas. Se trata de una condición de diseño (incorrecta) de subredes IP consistente en que el rango de direcciones de una subred contiene direcciones que están en el rango de otra subred.

Sucesor. En EIGRP, es la ruta mediante la cual se llega a la subred que tiene la mejor métrica y que debería incluirse en la tabla de enrutamiento IP.

Sucesor factible. En EIGRP, es una ruta que no es la mejor (una ruta factible) pero que se puede utilizar inmediatamente si falla la mejor ruta, sin dar lugar a un bucle. Estas rutas satisfacen la condición de viabilidad.

SVC. Circuito virtual conmutado. Es un CV que se configura dinámicamente cuando es necesario.

Switch. Es un dispositivo de red que filtra, envía e inunda tramas basándose en la dirección de destino de cada trama. El switch opera en la capa de enlace de datos del modelo de referencia OSI (Internetworking de sistemas abiertos).

Switch raíz. En STP, es el switch que gana las elecciones por tener el ID de puente más bajo; como consecuencia, este switch envía la BPDU de saludo de forma periódica (el tiempo predeterminado es de 2 segundos).

T

Tabla de vecinos. Para OSPF y EIGRP, se trata de una lista de routers que han alcanzado el estado de vecindad.

Temporizador de actualización. Es el intervalo de tiempo que regula la frecuencia con que un protocolo de enrutamiento envía sus actualizaciones de enrutamiento periódicas. Los protocolos de enrutamiento por vector de distancia envían actualizaciones de enrutamiento completas a cada intervalo de actualización.

TFTP. Protocolo trivial de transferencia de archivos (*Trivial File Transfer Protocol*). Es un protocolo de aplicación que permite la transferencia de archivos entre computadoras de una red, pero sólo posee unas pocas características, lo cual hace que el software tenga unos requisitos de almacenamiento muy reducidos.

Tipo de protocolo. Es un campo del encabezado IP que identifica el tipo de encabezado que sigue al encabezado IP, y que normalmente es un encabezado de capa 4, tal como TCP o UDP. Las ACLs pueden examinar el tipo de protocolo para identificar paquetes que tengan un determinado valor en este campo del encabezado.

Troncal. En las LANs de campus, se trata de un segmento Ethernet en el cual los dispositivos añaden una cabecera VLAN que identifica a la VLAN a la que pertenece la trama.

***Trunking*.** También se denomina *trunking* VLAN. Se trata de un método (que utiliza el protocolo ISL de Cisco o el protocolo 802.1Q del IEEE) para admitir múltiples VLANs que tengan miembros en más de un switch.

U

Unidad de datos del protocolo de puente. Véase BPDU.

V

Varianza. IGRP y EIGRP calculan sus métricas, así que las métricas de rutas diferentes hasta la misma subred rara vez tienen exactamente el mismo valor. El valor de varianza se multiplica por la métrica inferior cuando existen múltiples rutas hasta la misma subred. Si el producto es mayor que la métrica de otras rutas, se considera que las rutas tienen métricas "iguales", y se permite que se añadan múltiples métricas a la tabla de enrutamiento.

Vecino. En los protocolos de enrutamiento, es otro router con el cual un cierto router decide intercambiar información de enrutamiento.

Vector de distancia. Es la lógica que subyace al comportamiento de ciertos protocolos de enrutamiento interior, como RIP e IGRP. Los algoritmos de enrutamiento por vector de distancia piden a cada router que envíe su tabla de enrutamiento completa en todas las actualizaciones, pero sólo se la piden a sus vecinos. Los algoritmos de enrutamiento por vector de distancia son proclives a los bucles de enrutamiento, pero son más

sencillos computacionalmente que los algoritmos de enrutamiento por estado del enlace. También se denomina algoritmo de enrutamiento de Bellman-Ford.

Velocidad de acceso. Véase AR.

Velocidad de información suscrita. Véase CIR.

VLAN. Véase LAN virtual.

vlan.dat. Es el archivo predeterminado que se emplea para almacenar la base de datos de configuración de una VLAN en un switch de Cisco.

VLSM. Enmascaramiento o máscara de subredes de longitud variable (*Variable-length subnet mask* [*masking*]). Es la capacidad de especificar una máscara de subred diferente para un mismo número de red de clase A, B o C en diferentes subredes. VLSM puede ayudar a optimizar el espacio de direcciones disponible.

VoIP. Voz sobre IP (*Voice over IP*). Es el transporte de tráfico de voz dentro de paquetes IP a través de una red IP.

VPN. Véase Red privada virtual.

VTP. Véase Protocolo de *trunking* VLAN.

W

Web VPN. Es una herramienta que ofrece Cisco, mediante la cual el usuario puede emplear cualquier navegador web de uso habitual para efectuar una conexión segura empleando SSL con un servidor VPN web, que después se conecta con aplicaciones empresariales del usuario basadas en la Web; estas aplicaciones pueden admitir o no SSL.

Índice alfabético

Números

3DES (Triple DES), 536
802.1Q, *trunking* VLAN, 10-12
802.1w. Véase RSTP

A

ACL (Lista de control de acceso), 128
    basada en tiempos, 258
    coincidencias entre ACLs extendidas y estándares, 239
    con nombre, 247-249
    consideraciones de implementación, 254-255
    dinámicas, 257-258
    editar usando números de secuencia, 249-252
    extendida, 238-240
        configuración, 243-244
        ejemplos, 244-247
    gestión de la configuración, 247
    IP estándar, 227-230
        configuración, 233-234
        ejemplos, 234-238
    para acceder al control de acceso por Telnet y SSH, 253-254
    reflexivas, 255-256
    resolución de problemas, 294-296
    temas varios, 253
actualizaciones activadas, 324-325
AES (Estándar avanzado de cifrado), 536
AH (Encabezado de autenticación), 538, 539-540
aislar los problemas de interfaz, 121-122
algoritmo
    de actualización difuso (DUAL), 388
    de protocolo de enrutamiento, 310-311
ancho de banda, 385-386
antireproducción, 532
aplicaciones y sus números de puerto, 242
aprendizaje
    de direcciones IP de los servidores DNS, 605
    estado, 73
AR (Velocidad de acceso), 466
árbol de extensión. Véase también STP
    estados, 73
    funcionamiento del, 64-65
    necesidad del, 61-62
    opciones que influyen en su topología, 86-87
    qué hace el, 62-64
área interna, 347
ARP (Protocolo de resolución de direcciones), 163
        inverso, 500-501
ASN (número AS), 309
autenticación, 531
    fallos en PAP y CHAP, 453-455
autoconfiguración sin estado, 602-604
autoresumen, 215
    configuración, 219
    ejemplo, 215-216
    soporte del, 219
    y redes
        con clase separadas, 215
        discontinuas, 293-294

B

bases de datos
    de configuración VLAN, 19
    intercambio de, 352
BDR (Router designado de respaldo), 350
BECN (Notificación de la congestión retrospectiva), 483
BGP (Protocolo de gateway fronterizo), 309, 611
BID (ID de puente), 65
bidireccional, 346-347
BPDU
    Guard, configuración de, 93
    (Unidades de datos del protocolo de puente), 65
        Hello, 65-66
            campos, 66

C

cambios en la red, 70-73
CCNA Prep Center, 628
CDP, 120-121
CHAP, 444-446
    configuración y verificación, 447-448
CIDR, 553, 554
CIR (Velocidad de información suscrita), 467
circuito virtual, 466, 467-470
comandos
    area authentication, 359
    auto-cost reference-bandwidth, 359, 373
    access-class, 253
    access-list, 233, 235, 240, 243, 261
    bandwidth, 313, 359, 373, 526
    channel group, 105
    clear ip nat translations, 578
    debug
        eigrp, 405
        frame-relay lmi, 507
        ip
            nat, 578
            ospf, 374
        negotiation, 458
        ppp
            authentication, 453, 458
        spanning-tree events, 91
    delay, 404
    description, 504, 514
    encapsulation, 458, 496
        dot1q, 194
        frame-relay, 492, 493, 495, 526
        isl, 194
    erase startup-config, 20
    frame-relay
        interface-dlci, 494, 504, 507, 510, 521
        map, 494, 501, 521, 523, 526
    interface
        loopback, 364
        range, 26
        serial, 502, 527
    ip
        access-group, 261
        access-list, 261
            extended, 249
        address, 195
        authentication
            key-chain, 405
            key-mode, 405
        classless, 192
        default-network, 187-188, 195
        hello-interval, 40, 431
        hold-time, 405, 431
        nat
            inside, 565, 577
            outside, 565
        pool, 569, 577
        ospf, 359, 373
        route, 180, 185-187, 195
        summary-address, 211
    ipv6
        address, 601, 612, 622
        unicast-routing, 612, 622
    keepalive, 507, 526
    key chain, 397, 405
    maximum-paths, 373, 404
    name, 53
    network, 372, 404
    no ip
        access-list, 247
        classless, 192, 194
        subnet-zero, 195
    ping, 195, 266, 267, 512
        extendido, 182-184
    ppp
        authentication, 448, 458
            chap, 448
            pap, 448
    remark, 262
    router
        eigrp, 390, 404
        -id, 373
        ospf, 372
    show
        access-list, 262
        cdp
            entry, 121
            neighbors, 121
                detail, 121
        etherchannel, 106
        frame-relay
            lmi, 515, 527
            pvc, 507, 518
        interfaces, 54, 122, 133, 527
            description, 122
            status, 122
            switchport, 31
            trunk, 146

ip
access-list, 262
eigrp, 405
interfaces, 413, 431
neighbors, 422
interface, 262
nat
statistics, 567, 578
translations, 567, 578
ospf
interface brief, 413
neighbors, 424
protocols, 374, 405, 413, 431
route, 169, 186, 195, 287-288, 315, 405
eigrp, 431
ospf, 374
ipv6, 614, 622
port-security, 141, 142
running-configuration, 248
spanning-tree, 105
interface, 106
vlan, 88, 97, 106
vlan, 40, 54, 133
brief, 26, 133
vtp
password, 54
status, 40, 54
shutdown, 53
vlan, 53
spanning-tree
mode, 105
portfast, 105
vlan, 92, 105
static route, 208
switchport
access vlan, 26, 53
mode, 24, 53
nonnegotiate, 53
port-security violation, 128
trunk
allowed vlan, 32, 53
encapsulation, 28
voice vlan, 53
traceroute, 195, 266, 271-274
username, 458
variance, 400, 404
vlan, 53
vtp
domain, 53
password, 53
pruning, 53
con clase, 190
condición de viabilidad, 387
conformación de tráfico, 483
contiguo 48, 217
convergencia, 308, 336
con los protocolos por estado del enlace, 335
coste
cálculo del, 68
de puerto
de STP, 90-92
por VLAN, 87
CPU, 336
cuenta hasta infinito, 320-322
en una red redundante, 325-327

D

DCE (Equipo de comunicación de datos), 465, 466
DE (Posible para descarte), 484
decimal a binario, conversión, 651-653
denegar, 229
deny. Véase denegar
DES (Estándar de cifrado de datos), 536
descarte, 78
DHCP (Protocolo de configuración dinámica del host), 171
para IPv6, 598-599
diagramas de red, 120-121
verificar la exactitud, 137-139
dinámico deseable, modo, 29
direccionamiento
con clase, 189, 590
IP, 166-168
secundario, 174-176
IPv6, 597-598
privado, 555-556
sin clase, 189, 590
direcciones
de host IPv6, 599
IPv6, 605-609
distancia
administrativa, 313-315
factible, 385
informada, 385
distribución de claves, 537

DLCI (Identificador de conexión de enlace de datos), 467
asignación a una subinterfaz particular, 505
DNS (Sistema de denominación de dominios), 171, 564
DoS (Denegación de servicio), 41, 368
DR (router designado), 350
DTE (Equipo terminal de datos), 465, 466

E

Easy VPN, 540
EGP (Protocolo de gateway exterior), 309, 611
EIGRP (Protocolo de enrutamiento de gateway interior mejorado), 311, 377
autenticación, 397-400
comparación con OSPF, 389
conceptos, 380
configuración, 390-393
convergencia de, 386-387, 396-397
descubrimiento de vecinos, 380
intercambio de topologías, 380, 381-382
mensajes de actualización, 381
métrica, 393-394, 401-402
proceso de consulta y respuesta, 388
requisitos de vecindad, 421-423
ruta
máximas, 400-401
sucesora factible, 395-396
selección de rutas, 380
varianza, 400-401
vecinos, 380-381
Encapsulación
configuración en Frame Relay, 496-497
tipos de, 470-472
encriptación IPsec, 535-536
enlace
compartido, 81
con bucle, detección de, 442-443
de acceso, 465, 466
problemas, 513-515
punto a punto, 81
serie, resolución de problemas, 449-450
enrutamiento IP, 162-166
con y sin clase, 189, 190
envenenamiento de ruta, 319-320
envío de paquetes, resolución de problemas, 274-275
escenarios, 631-632
escucha, estado, 73
esfuerzo de diseño, 336
ESP (Sobrecarga de seguridad del encapsulado), 539-540
Estado
de la línea, 122
del enlace, 332
del protocolo, 122
EtherChannel, 74-75
configuración de, 93-94
EUI-64, formato, 599-601
extensión del ID de sistema, 87

F

FD. Véase distancia factible
FECN (Notificación explícita de la congestión), 483
filtrado, aislamiento de problemas de, 128-132
fragmentación y MTU, 172-174
Frame Relay, 461
asignación de direcciones, 497-500
búsqueda
de la subred conectada y de la interfaz de salida, 517
de los PVCs asignados a una interfaz, 518-519
configuración, 492, 493-494
determinación del PVC para llegar a un vecino, 519
direccionamiento
de capa 3, 477-481
en, 472-473
global en, 474-477
local en, 473-474
ejemplo de malla completa con una subred IP, 494-496
encapsulación, 496-497
entre extremos, 523-524
estado
de la subinterfaz, 521-522
de un PVC, 519-521
estándares, 467
manipulación de la difusión de capa 3, 482
mapeo estático, 501-502
números de subred desiguales, 524
problemas
de enlace de acceso, 513-515

de mapeo, 522-523
y estado de los PVCs, 516
red de malla parcial con
partes de malla completa, 508-511
una subred IP por VC, 502-505
resolución de problemas, 511-524
temas de la capa de red, 477
términos y conceptos, 466-467
velocidad y descartes, 482-483
verificación, 492, 506-508
visión general, 465-467

G

Global
externa, 559, 564
interna, 558, 559

H

HMAC (Código de autenticación de mensajes basado en la dispersión), 538
holddown, temporizador, 328-330
horizonte dividido, 322-323
con inversa envenenada, 325
host
inalcanzable, 268-269
palabra clave, 235

I

ICMP (Protocolo de mensajes de control en Internet), 171, 266-267
mensaje
de destino inalcanzable, 267-270
de tiempo excedido, 271
redirigir, 270-271
ID
de interfaz, 595, 599
de router, 345
de sistema, 86-87
IEEE 802.1d. Véase también STP
qué hace el árbol de extensión, 62-64
IEEE 802.1Q, 12-13
IGP (Protocolo de gateway interior), 309
comparativa de, 313
infinito, 319
información de estado, 598
integridad de los datos, 531
interfaz
buscar problemas de, 139-141
de acceso, 23, 26-27
de salida, 517
ejemplo de resolución de problemas, 418-420
estado de la, 288-289
loopback, 364
troncal, 26
internets privadas, 555
intra-área, 362
inversa envenenada, 324-325
IPsec, 534-535, 584
autenticación e integridad de mensajes, 537-539
encriptación, 535-536
implementación, consideraciones de, 540-541
intercambio de claves, 536-537
IPv4, 552-553
conservación de direcciones, 555
IPv6, 553, 581
agregación global de rutas, 586-588
aprendizaje de las direcciones IP de los servidores DNS, 605
asignación de direcciones de host, 599-604
autoconfiguración sin estado, 602-604
configuración, 612-615
estática de direcciones, 601-602
conversión entre IPv4 e IPv6, 618
DHCP para, 598-599
direccionamiento de unidifusión global, 585-586
direcciones, 605-606
de unidifusión, 606-608
formato EUI-64, 599-601
ID de interfaz, 599-601
multidifsión, 608-609
NDP, 604-605
pilas duales IPv4/Ipv6, 616
prefijos, 589-594, 597
protocolos, 597-598
de enrutamiento, 611-612
representación de direcciones, 588-589
router predeterminado, 604-605
transición a, 615
túneles, 616-617
ventajas que aporta, 584-585

ISATAP, 617
ISL (Enlace entre switches), 12
comparación con 802.1Q, 13-14
configuración, 177-180
trunking con, 10-11

K

keepalive, fallo de, 452-453

L

LANs
redundantes, problemas por no usar STP, 62
virtuales. Véase VLANs
LAPF (Procedimiento de acceso a través de un enlace), encabezado, 471
LCP (Protocolo para el control del enlace), 441-442
LMI (Interfaz de administración local), 465, 467
y tipos de encapsulación, 470-472
Local
exclusiva, 606
externa, 559, 564
interna, 558, 559
LSA
de enlace, 331
de router, 331
LSDB (Base de datos de estado del enlace), 331, 333, 344, 354
mantenimiento cuando el router es completamente adyacente, 352-353

M

máscara
de subred, 167
wildcard, 230-232
interpretación de una, 232-233
MCT (Túneles configurados manualmente), 617
MD5, 444, 538
mejores rutas, encontrar las, 333-334
mensaje
de control, 266
de destino inalcanzable, 267-270
métricas, 311-313
MIST (Instancias múltiples de árboles de extensión), 86
modo administrativo, 28
MST (Árboles de extensión múltiples), 86
MTU (Unidad máxima de transmisión), 172
requisito de igualdad, 429
multidifusión, 606

N

NAT (Conversión de direcciones de red), 227, 549
conceptos de conversión, 556
conversión de direcciones superpuestas, 563-565
dinámica, 560-561, 568-571
estática, 557-559
resolución de problemas, 565-575
sobrecarga con PAT, 561-563, 572-574
NAT-PT, 618
NBMA (Multiacceso sin difusión), 467
NDP (Protocolo de descubrimiento de vecindad), 602
descubrimiento del router predeterminado con, 604-605
no se puede fragmentar, 269
notación de prefijo, 167
notconnect y las especificaciones de cableado, 123-124
números de puerto
de las aplicaciones, 242
operadores para compararlos, 244
TCP y UDP, 240-243

O

operadores para comparar números de puerto, 244
OSPF (Primero la ruta libre más corta), 331
áreas de, 356-358
autenticación en, 368-370
con una sola área, 359-361
con varias áreas, 361-364
del ID de router, 364-365

búsqueda de vecinos con Hellos, 345-347
comparación con EIGRP, 389
configuración, 359
ventajas de las, 358
equilibrado de la carga, 370
escalado mediante un diseño jerárquico, 355-356
funcionamiento, 344
identificación de routers, 345
intercambio de la LSDB, 349-350
métrica (coste), 366-368
requisitos de vecindad, 424-427
selección de un router designado, 350-352
temporizadores Hello y muerto, 365-366
terminología de diseño, 357
tipos de autenticación, 369
vecinos en, 344-345

P

PAP, 444-446
configuración, 448
PAT (Conversión de direcciones de puerto), 561-563
permit. Véase permitir
permitir, 229, 245
pilas duales IPv4/Ipv6, 616
plan de estudio, 629
plano
de control, 111
de datos, 111
resolución de problemas, 117
ejemplo, 136-147
pasos a dar, 119
PortFast, 75, 81
configuración de, 93-94
PPP
autenticación en, 444-446
conceptos, 440
configuración básica, 446-447
detección de errores mejorada, 443
multienlace, 443-444
prefijo, 589-594
de sitio, 595
de subred, 595
terminología, 597
prioridad del switch, 90-92
privacidad, 531
proceso de envío, 117-132
protocolo
de enrutamiento, 307
con clase, 189, 201
exterior e interior, 309-310
funciones, 307-309
enrutable, 307
enrutado, 307
inalcanzable, 269
interfaces para un, 412-413
IPv6, 611-612
por estado del enlace, 330-331
por vector de distancia, 315-316
sin clase, 189, 201
puente
designado, 64
ID de, 65-66, 86
puerto
de respaldo, 80
designado, 64
determinación del, 100-101
elección en cada segmento LAN, 68-70
inalcanzable, 269-270
operativo, 65
prioridad del, 90
raíz, 64, 67
determinación del, 98-100
elección en cada switch, 67-68
PVC (Circuito virtual permanente), 465
asignado a una interfaz, 518-519
determinación del PVC para llegar a un vecino, 519
estado, 519-521
problemas y estado de un, 516
PVRST, 85
PVST+, 85

Q

QoS (Calidad de servicio), 35

R

RAM, 336
rango extendido, 13
RD. Véase distancia informada
Red

contigua, 217
inalcanzable, 268
separada, 217
redes con clase separadas, 216-219
resolución de problemas
aislamiento del problema 111, 115-116
análisis
de la causa raíz, 111, 116
del plano de
control, 114
datos, 112-114
/predicción de funcionamiento normal, 111-112
con la ruta
de envío, 278-281
inversa, 281-284
con los protocolos de enrutamiento, 410-412
con NAT, 565-575
de capa
1, 450-451
2, 451-452
3, 455-456
en el envío de paquetes, 274-275
en Frame Relay, 511-524
en las listas de acceso, 294-296
en una interfaz, 418-420
escenarios de ejemplo, 278-284
herramientas y pautas, 284-286
metodologías generales, 110-111
predicción del funcionamiento normal, 114-115
relacionados con los
hosts, 275-277
routers, 277-278
resumen manual de ruta, 208-212
estrategias del, 212-213
RID (ID de router), 345
RIP (Protocolo de información de enrutamiento), 186
router de respaldo, 351
RSTP (Protocolo de árbol de extensión rápido), 76-77
configuración de, 95-96
convergencia, 80-81
rápida, 81-83
estados de puerto, 78-79
roles de puerto, 79-80
tipos de enlace y contorno, 77-78
RTP (Protocolo de transporte fiable), 382
ruta
a subredes conectadas directamente, 174
conectadas en la subred cero, 177
de host, 455
envenenadas, 319-320
estáticas, 180-181
configuración de, 181-182
predeterminadas, 185-188
más específica, envío IP por la, 169
predeterminadas, 185-187
para la tabla de enrutamiento, 383-385

S

SDM (Administrador de seguridad de dispositivo), 552
seguridad de puerto, 128-132
buscar problemas de, 141-143
selección de ruta, 307
sincronización, 83
definición de, 18
solapamiento, 290
síntomas del, 291-293
SPF (Primero la ruta más corta), 333
de Dijkstra, 333-334
SSH, 253-254
SSL, 541
STA (Algoritmo de árbol de extensión), 64, 80
STP (Protocolo de árbol de extensión), 60.
Véase también árbol de extensión
cambios en la red, 70-73
características opcionales, 73-75
configuración y verificación, 84
convergencia de, 63, 101-102
determinación del switch raíz, 96-98
estados de puerto, 78
instancias múltiples, 84-86
razones para reenviar o bloquear, 65
resolución de problemas, 96
resumen de opciones de configuración, 88
seguridad en, 75-76
temporizadores, 71
stub area, 347
subinterfaz, estado de la, 521-522

subnetting IP, 166-168, 289
prácticas de, 630-631
vídeos de, 628
subredes
IP, 14-15
adición de, 205-207
VLSM solapadas, 201-203
sucesor, 387-388
factible, 387-388
SVC (Circuito virtual conmutado), 466
switch, soporte IP, 286-287
determinación del, 96-98
elección del, 66-67

T

tabla de enrutamiento IP
construcción de la, 353-354
más breves, 553-555
TCP, número de puerto, 240-243
Telnet, control de acceso por, 253-254
Temporizadores
Hello, 365-366
muerto, 365-366
Teredo, túnel, 67
TLS (Seguridad de la capa de transporte), 541
tododifusión, 606
trunking
aislamiento de problemas, 132
configuración, 28-32
para los teléfonos IP de Cisco, 34-35
túneles, 616-617
VPN, 532

U

UDP, número de puerto, 240-243, 561
unidifusión, 606
UTP, 124

V

Vecindad
estados de, 348-349
relaciones de, 420-421
requisitos de, 420, 421-425
Vecinos
problemas para llegar a hacerse, 347-348
resumen de los estados, 353
vector de distancia, 316-317
en una red estable, 317-318
prevenir bucles, 318-319
resumen, 330
velocidad
de acceso (AR), 466
de la interfaz, 125-128
VLANs
aislamiento de problemas, 132
asignación a una interfaz, 23-24
buscar problemas, 143-147
conceptos, 9-10
configuración, almacenamiento de la, 19-20
control en un troncal, 32-34
coste de puerto por VLAN, 87
creación, 23-24
de aparcamiento, 36
ejemplos, 24-28
etiquetado, 10
nativas, 14
y las subredes IP, 14-15
y troncales seguros
VLSM (Máscara de subred de longitud variable), 175, 199-200
configuración de, 207-208
cuándo utilizarla, 289
diseño de un escenario, 203-205
problemas, 289
resolución de problemas, 293
subredes VLSM solapadas, 289-291
VMPS Servidor de normas de gestión de VLAN), 24
VoIP, 34
VPN (Red privada virtual), 529
conceptos, 531-534
IPsec, 534-541
SSL, 541-543
tipos, 534
túnel, 532
VTP (Protocolo de *trunking* VLAN), 15-16
características, 22
comportamiento predeterminado, 88-90
configuración
de servidores y clientes, 37-40
predeterminada, advertencias al

cambiar la, 41-42
y verificación, 36
funcionamiento incorrecto, 43-48
modo
servidor y cliente, 16-18
transparente, 19, 42
problemas al conectar nuevos switches, 48-50
procedimientos comprobados, 50
pruning, 21-22
requisitos para que funcione entre dos switces, 18-19
resolución de problemas, 42-50
versiones de, 20-21

W

wildcard. Véase máscara *wildcard*